Configuring IPv6 Services

BayRS Version 12.00
Site Manager Software Version 6.00

Part No. 118428-A Rev. A
September 1997

Bay Networks

Bay Networks

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1997 Bay Networks, Inc.

All rights reserved. Printed in the USA. September 1997.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FN, FRE, GAME, LN, PPX, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, Bay•SIS, BayStack, BayStream, BCNX, BLNX, IP AutoLearn, SN, SPEX, Switch Node, System 5000, Bay Networks Press, and the Bay Networks logo are trademarks of Bay Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as “Software” in this Agreement).

BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR

PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

About This Guide

Before You Begin xvi
Conventions xvi
Acronyms xvii
Ordering Bay Networks Publications xviii
Bay Networks Customer Service xix
How to Get Help xix

Chapter 1
IPv6 Overview

IPv6 Header 1-1
IPv6 Addresses 1-2
Address Prefix 1-2
Interface ID 1-3
Anycast Address 1-3
Multicast Address 1-3
IPv4-Compatible Address 1-4
Address Formats 1-4
Tunnels 1-6
Static IPv4 Tunnel 1-6
Automatic IPv4 Tunnel 1-8
Semiautomatic IPv4 Tunnel 1-10
IPv6 Tunnels 1-10
Packet Forwarding 1-10
IPv6 Extension Headers 1-11
Neighbor Discovery 1-12
Address Autoconfiguration 1-12
RIPv6 1-13

Chapter 2
Starting IPv6 Services

Starting IPv6 2-1
Adding Neighbor Disovery to an IPv6 Interface 2-2
Adding RIPv6 to an IPv6 Interface 2-2

Chapter 3
Configuring and Customizing IPv6

Customizing IPv6 Globally 3-2
Enabling and Disabling Global IP 3-2
Configuring IPv6 in Not-Forwarding Mode 3-3
Supplying a Value for the Hop Limit Field 3-4
Specifying a Minimum Link MTU Size 3-5
Enabling and Disabling MTU Path Discovery 3-6
Specifying an MTU Path Timeout Period 3-7
Customizing an IPv6 Interface 3-8
Enabling and Disabling the Interface 3-9
Supplying a Description of the Interface 3-10
Supplying an Interface ID 3-11
Specifying the Circuit Name 3-12
Specifying the Link Layer Address 3-13
Specifying an MTU Size for the Link 3-14
Specifying the Size of the Forwarding Table 3-15
Configuring IPv6 on the Circuitless Interface 3-16
Enabling and Disabling Redirect Messages 3-17
Configuring ICMP Error Messages 3-18
Enabling and Disabling TR End Station Support 3-19
Specifying an SMDS Group Address 3-20
Specifying Frame Relay Broadcast DLCI 3-21
Specifying Frame Relay Multicast DLCI 3-22
Configuring a Tunnel on the Interface 3-23
Configuring an IPv6 Interface as a Tunnel End Point 3-24
Specifying a Tunnel Type 3-25
Specifying a Local IPv4 Address 3-27
Specifying a Remote IPv4 Address 3-28
Specifying a Local IPv6 Index 3-29

Specifying a Remote IPv6 Address 3-30
Configuring an IPv6 Address Prefix 3-31
Associating a Prefix with an interface ID 3-32
Enabling and Disabling Use of the Prefix 3-33
Supplying an Address Prefix 3-34
Specifying the Length of the Prefix 3-35
Specifying a Routing Preference 3-36
Specifying a Cost 3-37
Configuring the Prefix for On-Link Determination 3-38
Enabling Autonomous Address Configuration 3-39
Supplying a Preferred Lifetime Value 3-40
Supplying a Valid Lifetime Value 3-41
Customizing IPv6 Neighbor Discovery 3-42
Enabling and Disabling Neighbor Discovery 3-43
Controlling Router Advertisements 3-44
Controlling Address Autoconfiguration 3-45
Controlling Nonaddress Autoconfiguration 3-46
Specifying a Neighbor Reachability Time 3-47
Specifying a Retransmission Time For Neighbor Solicitations 3-48
Specifying a Maximum Hop Limit for ND Advertisements 3-49
Specifying a Minimum Time for Unsolicited Advertisements 3-50
Specifying a Maximum Time for Unsolicited Advertisements 3-51
Specifying a Lifetime for the Default Router 3-52
Configuring Address Duplication Detection 3-53
Defining an IPv6 Adjacent Node 3-54
Enabling and Disabling the Adjacent Node Definition 3-55
Supplying the Physical Address of the Adjacent Node 3-56
Specifying the Link Layer Encapsulation Type 3-57
Specifying a Route Preference Value 3-58
Specifying the Cost 3-59
Supplying the WAN Address of the Adjacent Node 3-60
Configuring an IPv6 Static Route 3-61
Associating the Static Route with an Interface 3-61
Enabling and Disabling the Static Route 3-62
Supplying the Destination IPv6 Address Prefix 3-63

Specifying the Prefix Length 3-64
Supplying the IPv6 Next-Hop Address 3-65
Specifying a Route Preference Value 3-66
Specifying the Cost 3-67
Configuring a Static Default Route 3-68
Configuring a Black Hole 3-68

Chapter 4
Configuring RIPv6

Enabling and Disabling RIP 4-2
Supplying RIP Updates 4-3
Receiving RIP Updates 4-4
Supplying a Default Route 4-5
Listening for a Default Route 4-6
Specifying the Update Mode 4-7
Specifying an Interval for Update Broadcasts 4-8
Specifying a Timeout Period for an Unreachable Network 4-9
Specifying a Hold Down Time 4-10
Sending Triggered Updates 4-11
Specifying the RIPv6 Diameter 4-12
Configuring RIPv6 Policies 4-13
Configuring a RIPv6 Accept Policy 4-14
Configuring a RIPv6 Announce Policy 4-16

Appendix A
Site Manager Parameters for IP Version 6

IPv6 Global Parameters A-1
IPV6 Interface Parameters A-3
IPv6 Prefix Parameters A-11
IPv6 Neighbor Discovery Parameters A-14
IPv6 Adjacent Node Parameters A-18
IPv6 Static Route Parameters A-20
RIP IPv6 Interface Parameters A-22
RIPv6 Accept Policy Parameters A-26
RIPv6 Announce Policy Parameters A-31

Index

Figures

Figure 1-1. 128-Bit IPv6 Address Format 1-2
Figure 1-2. Multicast Address Format 1-3
Figure 1-3. IPv4-Compatible Unicast Address Format 1-4
Figure 1-4. Configured IPv4 Static Tunnel 1-7
Figure 1-5. Automatic IPv4 Tunnel 1-9
Figure 1-6. IPV6 Header and Extension Headers 1-11

About This Guide

If you are responsible for configuring IPv6 and RIPv6, you need to read this guide.

If you want to	Go to
Learn about IPv6 concepts and services	Chapter 1
Start IPv6 services on the router	Chapter 2
Configure and Customize IPv6	Chapter 3
Configure and customize RIPv6	Chapter 4
Obtain information about Site Manager parameters (this is the same information you obtain using Site Manager online Help)	Appendix A

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation manual that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks® Site Manager and router software. For instructions, see *Upgrading Routers from Version 7–11.xx to Version 12.00*.

Conventions

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: if command syntax is **ping** *<ip_address>*, you enter **ping 192.32.10.12**
bold text	Indicates text that you need to enter, command names, and buttons in menu paths. Example: Enter **wfsm &**
	Example: Use the **dinfo** command.
	Example: ATM DXI > Interfaces > **PVCs** identifies the PVCs button in the window that appears when you select the Interfaces option from the ATM DXI menu.
brackets ([ ])	Indicate optional elements. You can choose none, one, or all of the options.
ellipsis points	Horizontal (. . .) and vertical (⋮) ellipsis points indicate omitted information.
italic text	Indicates variable values in command syntax descriptions, new terms, file and directory names, and book titles.
quotation marks (“ ”)	Indicate the title of a chapter or section within a book.

`screen text`	Indicates data that appears on the screen. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Separates menu and option names in instructions and internal pin-to-pin wire connections. Example: Protocols > AppleTalk identifies the AppleTalk option in the Protocols menu. Example: Pin 7 > 19 > 20
vertical line (|)	Indicates that you enter only one of the parts of the command. The vertical line separates choices. Do not type the vertical line when entering the command. Example: If the command syntax is **show at routes** | **nets**, you enter either **show at routes** or **show at nets**, but not both.

Acronyms

AUI	Attachment Unit Interface
BootP	Bootstrap Protocol
BRI	Basic Rate Interface
CCITT	International Telegraph and Telephone Consultative Committee (now ITU-T)
CSMA/CD	carrier sense multiple access with collision detection
DLCMI	Data Link Control Management Interface
GUI	graphical user interface
HDLC	high-level data link control
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ITU-T	International Telecommunications Union-Telecommunications (formerly CCITT)
LAN	local area network
MAC	media access control
MAU	media access unit
MDI-X	media-dependent interface with crossover
NBMA	nonbroadcast multi-access

OSI	Open Systems Interconnection
OSPF	Open Shortest Path First (Protocol)
PPP	Point-to-Point Protocol
SMDS	switched multimegabit data service
SNMP	Simple Network Management Protocol
STP	shielded twisted-pair
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	Telecommunication Network
TFTP	Trivial File Transfer Protocol
TPE	twisted-pair Ethernet
UTP	unshielded twisted-pair
WAN	wide area network

Ordering Bay Networks Publications

To purchase additional copies of this document or other Bay Networks publications, order by part number from Bay Networks Press™ at the following numbers:

- Phone--U.S./Canada: 888-422-9773
- Phone--International: 510-490-4752
- FAX--U.S./Canada and International: 510-498-2609

The Bay Networks Press catalog is available on the World Wide Web at *support.baynetworks.com/Library/GenMisc*. Bay Networks publications are available on the World Wide Web at *support.baynetworks.com/Library/tpubs*.

Bay Networks Customer Service

You can purchase a support contract from your Bay Networks distributor or authorized reseller, or directly from Bay Networks Services. For information about, or to purchase a Bay Networks service contract, either call your local Bay Networks field sales office or one of the following numbers:

Region	Telephone number	Fax number
United States and Canada	800-2LANWAN; then enter Express Routing Code (ERC) 290, when prompted, to purchase or renew a service contract 978-916-8880 (direct)	978-916-3514
Europe	33-4-92-96-69-66	33-4-92-96-69-96
Asia/Pacific	61-2-9927-8888	61-2-9927-8899
Latin America	561-988-7661	561-988-7550

Information about customer service is also available on the World Wide Web at *support.baynetworks.com*.

How to Get Help

If you purchased a service contract for your Bay Networks product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

If you purchased a Bay Networks service program, call one of the following Bay Networks Technical Solutions Centers:

Technical Solutions Center	Telephone number	Fax number
Billerica, MA	800-2LANWAN	978-916-3514
Santa Clara, CA	800-2LANWAN	408-495-1188
Valbonne, France	33-4-92-96-69-68	33-4-92-96-69-98
Sydney, Australia	61-2-9927-8800	61-2-9927-8811
Tokyo, Japan	81-3-5402-0180	81-3-5402-0173

Chapter 1
IPv6 Overview

This overview of IP Version 6 covers the following topics:

Topic	Page
IPv6 Header	1-17
IPv6 Addresses	1-18
Tunnels	1-21
Packet Forwarding	1-25
IPv6 Extension Headers	1-26
Neighbor Discovery	1-27
Address Autoconfiguration	1-27
RIPv6	1-28

IPv6 Header

The IPv6 protocol defines the header used by IPv6 nodes (hosts and routers) to deliver a data packet from a sender to one or more destinations.

The *IPv6 header* supplies a 128-bit source address and a 128-bit destination address for a data packet. The header also includes a flow control field that an IPv6 host can use to label packets that require special handling by IPv6 routers -- for example, packets that require a real-time service.

IPv6 Addresses

An IPv6 address consists of 128 bits that identify an interface or a set of interfaces. The address consists of two parts: an address prefix and an IPv6 interface ID. The first 3 bits of the address indicate the type of address that follows -- a unicast address, for example.

Figure 1-1 shows the basic parts of an IPv6 address.

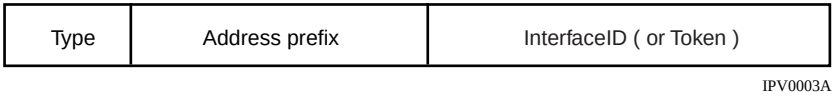

Figure 1-1. 128-Bit IPv6 Address Format

Address Prefix

The *address prefix* consists of one or more *aggregator addresses*. These addresses are listed in the hierarchical order of the organizations that issue them.

- At the top of the hierarchy, international registries assign blocks of addresses to *top-level aggregators* (TLAs). TLA addresses provide the public transit points where long-haul service providers establish peer connections.
- TLAs allocate blocks of address to the *next-level aggregators* (NLAs), the large Internet service providers and global corporate networks.
- An NLA that is a service provider further allocates its addresses to its subscribers, the lowest-level aggregators, the *site-level aggregators* (SLAs).

TLA and NLA addresses are part of the public Internet topology. SLA addresses are part of private site-level topologies.

Interface ID

The *interface ID* or *token* is a unique number identifying an IPv6 node (a host or a router). For stateless autoconfiguration (see “Address Autoconfiguration” on page 1-27), this ID is 64 bits long.

In IPv6 stateless autoconfiguration, the interface ID is derived by a formula that uses the link layer 48-bit MAC address. (In most cases, the interface ID is a 64-bit token that contains the 48-bit MAC address.) This means that to the extent that the MAC address is unique, the IPv6 interface ID is unique.

If you configure tokens or MAC addresses (or both) manually, there need be no relation between the MAC address and the token. A manually configured token may also be longer or shorter than 64 bits.

Anycast Address

An IPv6 *anycast address* is a unicast address identifying a group of IPv6 nodes that share a common variable-length address prefix. A packet bearing an anycast address is delivered to one node in the group.

Multicast Address

An IPv6 *multicast address* identifies a group of nodes. A packet bearing a multicast address is delivered to all members of the group. (The function of IPv4 broadcast addresses has been superseded by IPv6 multicast addresses.)

Figure 1-2 shows the format of an IPv6 multicast address.

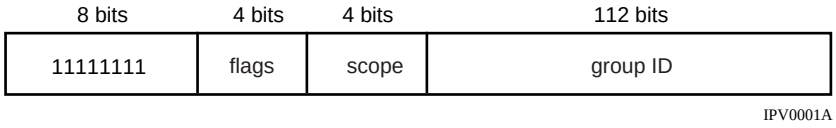

Figure 1-2. Multicast Address Format

A value of FF (11111111) in the 8 high-order bits of an IPv6 address indicates that the address specifies a multicast group. The 4-bit *flags* field indicates whether the group is permanent or transient. The 4 -bit *scope* field indicates the scope of the group specified in the 112-bit *group ID* field.

IPv4-Compatible Address

The IPv4-compatible address, which includes an IPv4 address in the low-order 32 bits, is intended for IPv6 nodes that need to interoperate with IPv4 nodes. Figure 1-3 shows the format of an IPv4-compatible address.

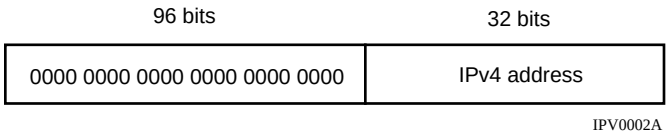

Figure 1-3. IPv4-Compatible Unicast Address Format

Address Formats

The format for representing an IPv6 address is

n:*n*:*n*:*n*:*n*:*n*:*n*:*n*

n is the hexadecimal representation of 16 bits in the address. For example:

FF01:0:0:0:0:0:0:43

Each nonzero field must contain at least one numeral. Within a given hexadecimal field, however, leading 0s are not required.

Certain classes of IPv6 addresses commonly include multiple contiguous fields containing hexadecimal 0. Our sample address includes five contiguous fields containing 0. These fields can be represented by double colons (::). For example:

FF01::43

A double colon can also be used to compress the leading zero fields in a hexadecimal address. A double colon can appear once in an address.

An IPv4-compatible address combines hexadecimal and decimal values as follows:

x.x.x.x.x.x.d.d.d.d

x:x:x:x:x:x is a hexadecimal representation of the six high-order 16-bit pieces of the address and *d.d.d.d* is a decimal representation of the four 8-bit pieces of the address. For example:

0:0:0:0:0:0:13.1.68.3

or

::13.1.68.3

Tunnels

Tunneling is a forwarding technique in which a packet is encapsulated inside another packet.

IPv6 supports two kinds of encapsulating tunnels: IPv4 tunnels and IPv6 tunnels.

In IPv4 tunneling, a router running both IPv6 and IPv4 encapsulates an IPv6 packet within an IPv4 packet. This technique allows IPv6 nodes in noncontiguous IPv6 regions to forward messages through an intervening region of IPv4 nodes.

In IPv6 tunneling, a router running IPv6 encapsulates an IPv6 packet in another IPv6 packet. This section covers the following topics:

Topic	Page
Static IPv4 Tunnel	1-22
Automatic IPv4 Tunnel	1-23
Semiautomatic IPv4 Tunnel	1-25
IPv6 Tunnels	1-25

Static IPv4 Tunnel

A *static tunnel* -- also called a *configured tunnel* -- is a mechanism for forwarding any IPv6 packet through an IPv4 region. Figure 1-4 shows a static tunnel between an IPv4 interface on router C and an IPv4 interface on router D. (Note that routers C and D are running both IPv4 and IPv6).

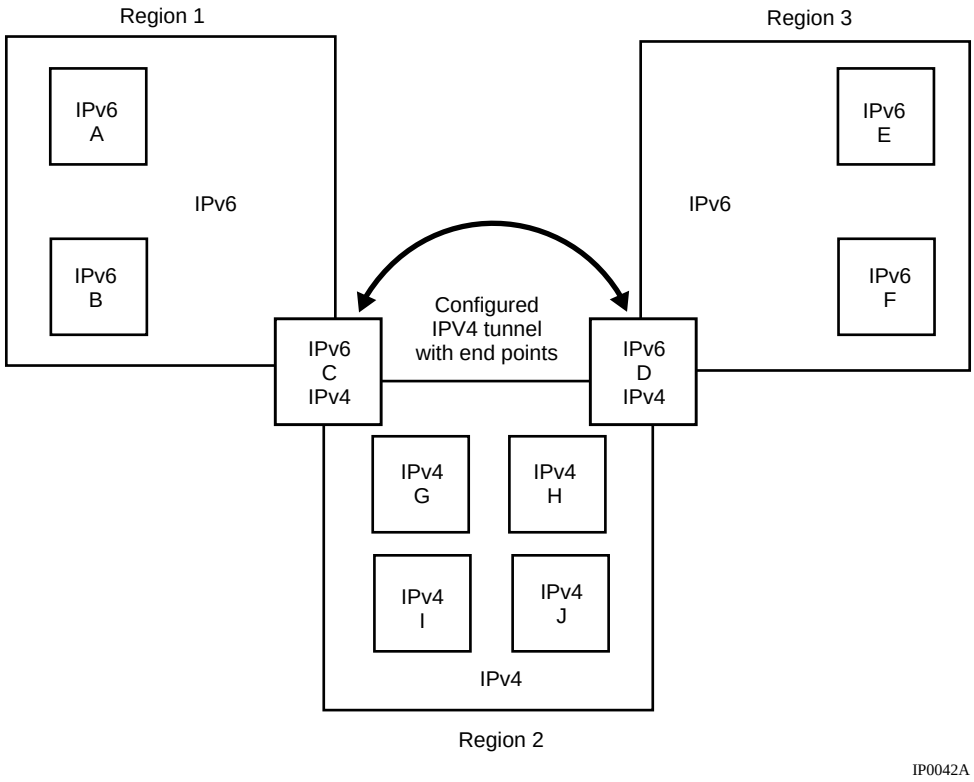

Figure 1-4. Configured IPv4 Static Tunnel

In Figure 1-4, for example, a user connected to router B in Region 1 sends a packet addressed to a user on router F in Region 3. The following steps occur:

1. Router C receives the IPv6 packet and determines that it must be forwarded out its tunnel interface.

2. Router C encapsulates the IPv6 packet in an IPv4 header.

   The source address in the IPv4 header is the IPv4 address of the local tunnel interface on router C. The destination address is the IPv4 address of the remote tunnel interface on router D.

3. Using the IPv4 header, intermediate IPv4 routers in Region 2 forward the encapsulated packet through the IPv4 region to router D.

4. Router D decapsulates the packet (removing the IPv4 header) and forwards the original IPv6 packet to router F.

After you have configured the IPv4 interfaces on the end point routers, the tunnel becomes a permanent point-to-point link in the IPv6 topology.

Automatic IPv4 Tunnel

An *automatic tunnel* is a mechanism for forwarding unicast IPv6 packets that use the IPv4-compatible address format. All routers in IPv6 regions that use automatic tunneling must run both IPv6 and IPv4.

IPv6 creates the tunnel dynamically as needed for the purpose of forwarding an IPv6 packet through multiple IPv4 and IPv4/IPv6 routers.

In Figure 1-5, for example, a user connected to router B in Region 1 wants to send an IPv6 packet to a user on router J in Region 3.

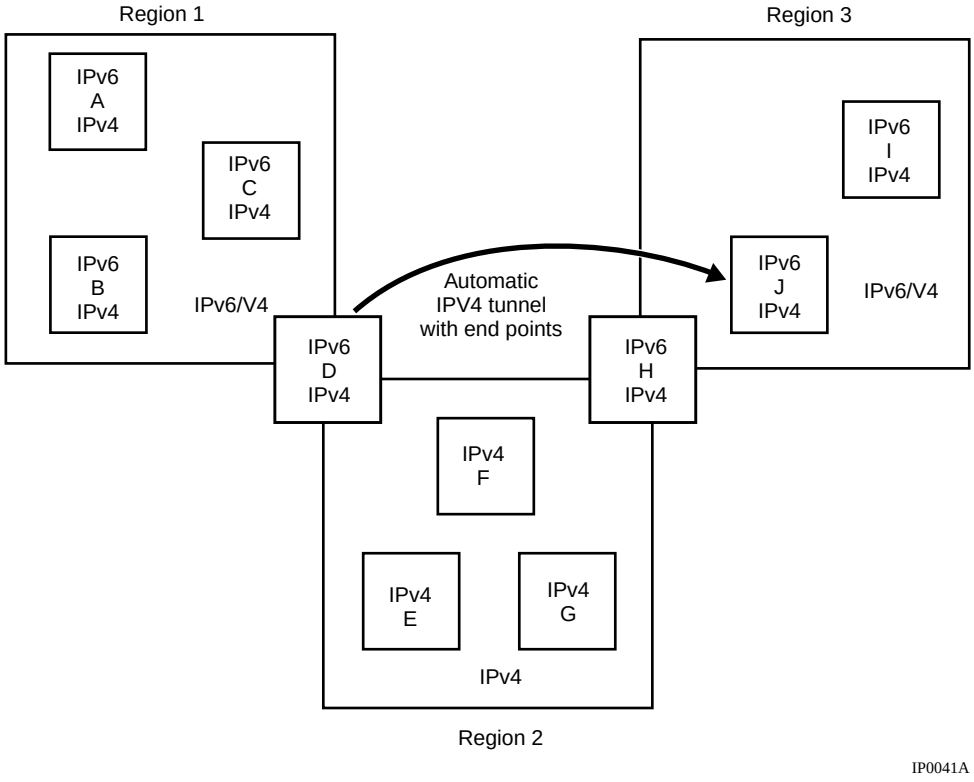

Figure 1-5. Automatic IPv4 Tunnel

The following steps occur:

1. Router D receives the packet and determines that the next hop requires an automatic tunnel.
2. Router D encapsulates the packet in an IPv4 header.

   The source address in the IPv4 header is the IPv4 address of the local tunnel interface on node D.

   The destination address is the IPv4 address contained in the IPv4-compatible IPv6 address. This is the address of an IPv4 interface on router J.
3. IPv4 routers in Region 2 forward the packet to Region 3.
4. IPv4/ IPv6 router in Region 3 forward the IPv4 packet to router J.

5. Router J decapsulates the packet.

Note that unlike a configured tunnel, which is a permanent point-to-point link in the IPv6 topology, an automatic tunnel is a dynamic mechanism, created by the encapsulating end point for the purpose forwarding an IPv6 packet. After the packet reaches its destination, the automatic tunnel no longer exists.

Semiautomatic IPv4 Tunnel

A semiautomatic tunnel acts as a static tunnel for outgoing traffic and as an automatic (multipoint-to-point) tunnel for incoming traffic.

IPv6 Tunnels

Like an IPv4 tunnel, an IPv6 tunnel can be a static tunnel, an automatic tunnel, or a semiautomatic tunnel.

Packet Forwarding

IPv6 forwards

- Unicast packets not addressed to itself.
- Packets with predefined multicast addresses.
- Packets addressed to itself that include a routing source extension header. The extension header specifies a list of one or more intermediate nodes that define a path for the packet to follow through the network to its destination.

IPv6 processes packets that are addressed to itself (with the exception of packets that contain a routing option extension header). IPv6 recognizes the following addresses as identifying itself:

- A unicast address assigned to the router
- A loopback address used by a node to send an IPv6 datagram to itself
- An all-nodes or all-hosts multicast address
- An anycast address assigned to the router

IPv6 Extension Headers

IPv6 *extension headers* describe processing options. Each extension header contains a separate category of options. A packet can include zero or more extension headers (Figure 1-6).

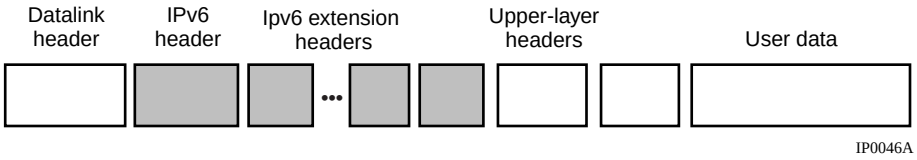

Figure 1-6. IPV6 Header and Extension Headers

IPv6 examines the destination address in the main header of each packet it receives to determine whether the router is the packet's destination or an intermediate node in the packet's data path.

- If the router is the destination of the packet, IPv6 examines the header extensions that contain options for destination processing.
- If the router is an intermediate node, IPv6 examines the header extensions that contain forwarding options.

By examining only the extension headers that apply to the operations it performs, IPv6 reduces the amount of time and processing resources required to process a packet.

IPv6 defines the following extension headers:

- The *source routing* extension header contains a list of one or more intermediate nodes that define a path for the packet to follow through the network to its destination. The packet source creates this list. This function is similar to IPv4 source routing options.
- The *fragmentation* extension header is used by an IPv6 source to send packets larger than the size specified for the path MTU.
- The *authentication* extension header and the *security encapsulation* extension header, used singly or together, provide security services for IPv6 datagrams.

- The *hop-by-hop* extension header contains optional information that must be examined by all intermediate IPv6 routers between the source and the destination.
- The *end-to-end* extension header contains optional information that must be examined by the destination node.

Neighbor Discovery

Neighbor discovery (ND) allows IPv6 nodes on the same link to discover link layer addresses and to obtain and advertise various network parameters and reachability information. ND combines the services provided for IPv4 by the Address Resolution Protocol (ARP) and router discovery.

Address Autoconfiguration

Typically, to start the process of autoconfiguration, a node

- Self-configures a link-local address to use temporarily. The host can form this address by adding a generic local address prefix to a unique token (typically, the host's IEE LAN interface address).
- Sends out an ND message to the address to ensure that it is unique. If no ND message comes back, the address is unique. If a message comes back indicating that the link-local address is already in use, the host uses a different token (for example, an administrative token or a randomly generated token).
- Uses the IPv6 multicast service to send out an ND router solicitation request, using the new link-local address as a source address. Unlike the broadcast ARPs of IPv4, ND multicast solicitations are not necessarily processed by all nodes on the link. IPv6 defines several permanent multicast groups for finding resources on a local node or link, including an all-routers group, an all-hosts group, and a Dynamic Host Configuration Protocol (DHCP) server group.

Routers respond to the solicitation messages from hosts with a unique router advertisement that includes prefix information indicating a valid range of addresses for the subnet. Routers can also send these advertisements periodically to local multicast groups, whether or not they receive solicitations.

Using the router advertisement message that it sends in response to a solicitation from a host, an IPv6 router can control whether the host uses *stateful* or *stateless* autoconfiguration.

In stateful autoconfiguration, the host contacts a DHCP or similar address server, which assigns an address from a manually administered list.

In stateless autoconfiguration, a host can automatically configure its own IPv6 address without the help of a stateful address server. The host uses the globally valid address prefix information in the router advertisement message to create its own IPv6 address. The host concatenates the valid prefix with its link layer address (or a similar unique token) to create an IPv6 address.

RIPv6

RIPv6 -- the Routing Information Protocol for IPv6 -- is a distance-vector protocol that enables IPv6 routers in the same autonomous system to exchange routing information by means of periodic RIP updates. Routers transmit their own RIPv6 updates to neighboring networks and listen for RIPv6 updates from the routers on those neighboring networks. Routers use the information in the RIPv6 updates to keep their internal routing tables current. For RIPv6, the “best” path to a destination is the shortest path (the path with the fewest hops). RIPv6 computes distance as a metric, usually the number of hops (or routers) from the origin network to the target network.

RIPv6 is described in Chapter 4.

Chapter 2
Starting IPv6 Services

Starting IPv6

Before you can choose a protocol to run on the router, you must configure a circuit that the protocol can use as an interface to an attached network. For information and instructions, see *Configuring Ethernet, FDDI, and Token Ring Services* or *Configuring WAN Line Services*.

When you have successfully configured the circuit, the Select Protocols window opens. Proceed as follows:

Site Manager Procedure	
You do this	**System responds**
1. In the Select Protocols window, choose **IPv6.**	The Configure Interfaces window opens.
2. Click on **OK** to accept default values for IPv6 parameters.	You return to the Configuration Manager window.

IPv6 is now configured on this interface and slot with default values for all global and interface parameters. You customize IPv6 by modifying IPv6 parameters as described in Chapter 3.

Adding Neighbor Discovery to an IPv6 Interface

Use Site Manager to add Neighbor Discovery to an IPv6 interface as follows.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Neighbor Discovery**.	The List IPv6 Neighbor Discovery window opens.
4. Choose **Add**.	The Values Selection window opens.
5. Choose the IPv6 interface to which you want to add Neighbor Discovery, and click on **OK**.	The Values Selection window closes and the interface you chose appears in the List IPv6 Neighbor Discovery window.
6. Click on **Apply** and **Done** to accept default values for Neighbor Discovery parameters.	You return to the Configuration Manager window.

To customize the Neighbor Discovery values, go to page 3-42.

Adding RIPv6 to an IPv6 Interface

Use Site Manager to add RIPv6 to an IPv6 interface as follows.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **RIPv6 Interfaces**.	The RIPv6 Interfaces window opens.
4. Choose **Add**.	The IPv6 Indexes window opens.
5. Choose the index value for the IPv6 interface to which you want to add RIPv6.	The RIPv6 Interfaces window reopens.
6. Click on **Apply** and **Done** to accept default values for RIPv6 parameters.	You return to the Configuration Manager window.

To customize the RIPv6 values, go to Chapter 4.

Chapter 3
Configuring and Customizing IPv6

You configure and customize IPv6 by setting IPv6 parameters as described under the following topics:

Topic	Page
Customizing IPv6 Globally	3-2
Customizing an IPv6 Interface	3-8
Configuring a Tunnel on the Interface	3-23
Configuring an IPv6 Address Prefix	3-31
Customizing IPv6 Neighbor Discovery	3-42
Defining an IPv6 Adjacent Node	3-54
Configuring an IPv6 Static Route	3-61
Configuring a Static Default Route	3-68
Configuring a Black Hole	3-68

Customizing IPv6 Globally

When you configure an IPv6 interface, IPv6 runs on the router with default values for all global parameters. You customize IPv6 on the router by modifying global parameters as described under the following topics:

Topic	Page
Enabling and Disabling Global IP	3-2
Configuring IPv6 in Not-Forwarding Mode	3-3
Supplying a Value for the Hop Limit Field	3-4
Specifying a Minimum Link MTU Size	3-5
Enabling and Disabling MTU Path Discovery	3-6
Specifying an MTU Path Timeout Period	3-7

Enabling and Disabling Global IP

By default, IPv6 is enabled on the router.

You can use the following Site Manager procedure to change the state as required.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **IPv6 Global**.	The Edit IPv6 Global Parameters window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-1.	
5. Click on **OK**.	Site Manager returns you to the Configuration Manager window.

Configuring IPv6 in Not-Forwarding Mode

By default IPv6 forwards all packets that are not addressed to itself.

You can use the following Site Manager procedure to specify whether this entity is acting as an IPv6 router in respect to the forwarding of datagrams. Ipv6 routers forward received datagrams that are not addressed to itself. IPv6 hosts do not forward datagrams (except those source-routed via the host).

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **IPv6 Global**.	The Edit IPv6 Global Parameters window opens.
4. Set the **Forwarding** parameter. Click on **Help** or see the parameter description on page A-1.	
5. Click on **OK**.	Site Manager returns you to the Configuration Manager window.

Supplying a Value for the Hop Limit Field

The IPv6 header includes a hop limit field set by the originating router (the source node). Each intermediate node (that is, each node that receives and forwards the packet) decrements the hop-limit value by one. When the hop-limit value decrements to zero, the packet is discarded. (The IPv6 hop-limit value serves the same function as the IPv4 time-to-live value.)

By default, IPv6 inserts a value of 64 into the Hop Limit field of the header of datagrams originated at the router.

If the transport layer protocol supplies a hop-limit value, IPv6 uses that value.

You can use the following Site Manager procedure to specify a hop-limit value from 0 to 255.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **IPv6 Global**.	The Edit IPv6 Global Parameters window opens.
4. Set the **Default Hop** parameter. Click on **Help** or see the parameter description on page A-2.	
5. Click on **OK**.	Site Manager returns you to the Configuration Manager window.

Specifying a Minimum Link MTU Size

Each link in the IPv6 internet has a maximum transmission unit (MTU) size. The MTU size is expressed in bytes.

IPv6 uses MTU path discovery to learn the MTU size used in the IPv6 internet. (For instructions and information, see “Enabling and Disabling MTU Path Discovery” on page 3-6.)

By default, if MTU path discovery is disabled, IPv6 generates packets with an MTU size of 576 bytes.

By changing this parameter, you can control the maximum size of packets that can be generated by this router if MTU path discovery is disabled.

You can use the following Site Manager procedure to specify a minimum link MTU size from 296 to 65535 bytes.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **IPv6 Global**.	The Edit IPv6 Global Parameters window opens.
4. Set the **Minimum Link MTU** parameter. Click on **Help** or see the parameter description on page A-2.	
5. Click on **OK**.	Site Manager returns you to the Configuration Manager window.

Enabling and Disabling MTU Path Discovery

Each link in the IPv6 internet has an MTU size, which is expressed in bytes.

By default IPv6 uses MTU path discovery to learn the MTU size for the IPv6 internet.

Disable this feature if you want to use the Minimum Link MTU parameter to control the maximum size of self-generated packets.

You can use the following Site Manager procedure to enable and disable MTU path discovery support for self-originated packets.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **IPv6 Global**.	The Edit IPv6 Global Parameters window opens.
4. Set the **MTU Discovery** parameter. Click on **Help** or see the parameter description on page A-2.	
5. Click on **OK**.	Site Manager returns you to the Configuration Manager window.

Specifying an MTU Path Timeout Period

By default, a router that has learned a link MTU value through MTU path discovery considers the value to be valid for 10 minutes.

You can use the following Site Manager procedure to specify a timeout period from 1 minute to 71582788 minutes or to disable the feature (by specifying 0).

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **IPv6 Global**.	The Edit IPv6 Global Parameters window opens.
4. Set the **MTU Timeouts** parameter. Click on **Help** or see the parameter description on page A-3.	
5. Click on **OK**.	Site Manager returns you to the Configuration Manager window.

Customizing an IPv6 Interface

When you configure an IPv6 interface on a circuit, IPv6 runs with default values for all interface parameters. You customize the IPv6 interface by modifying parameters as described under the following topics:

Topic	Page
Enabling and Disabling the Interface	3-9
Supplying a Description of the Interface	3-10
Supplying an Interface ID	3-11
Specifying the Circuit Name	3-12
Specifying the Link Layer Address	3-13
Specifying an MTU Size for the Link	3-14
Specifying the Size of the Forwarding Table	3-15
Configuring IPv6 on the Circuitless Interface	3-16
Enabling and Disabling Redirect Messages	3-17
Configuring ICMP Error Messages	3-18
Enabling and Disabling TR End Station Support	3-19
Specifying an SMDS Group Address	3-20
Specifying Frame Relay Broadcast DLCI	3-21
Specifying Frame Relay Multicast DLCI	3-22

Enabling and Disabling the Interface

By default, IPv6 is enabled on the interface:

You can use the following Site Manager procedure to disable and reenable IPv6 on the interface as required.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying a Description of the Interface

You can use the following Site Manager procedure to enter a description of the IPv6 interface from 1 to 255 characters.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Interface Description** parameter. Click on **Help** or see the parameter description on page A-3.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying an Interface ID

The interface ID -- also called the token -- is a unique number identifying an IPv6 node (a host or a router). This ID is 64 bits long for stateless autoconfiguration.

In IPv6 stateless autoconfiguration, the interface ID is derived by a formula that uses the link layer 48-bit MAC address. (In most cases, the interface ID is a 64-bit number that contains the 48-bit MAC address.)

If you elect to configure interface tokens or MAC addresses (or both) manually, there need not be any relation between the MAC address and the token. A manually configured token may also be longer or shorter than 64 bits.

You can use the following Site Manager procedure to supply a different interface ID from one to six characters.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Interface Token** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Circuit Name

By default, IPv6 uses the circuit name you specified when you configured the interface.

You can configure an interface as the circuitless interface or as a tunnel end point.

- To configure the interface as the circuitless interface, set this parameter with a value greater than 1023 (the highest valid circuit number).
- To configure the interface as a tunnel end point, set this parameter to 0.

You can use the following Site Manager procedure to set the Circuit Name parameter.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Circuit Name** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Link Layer Address

By default, IPv6 uses the 48-bit MAC address of the interface on which this interface is configured as the link layer address.

You can use the following Site Manager procedure to supply a link layer address.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Link Layer Address** parameter. Click on **Help** or see the parameter description on page A-4.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying an MTU Size for the Link

By default, IPv6 uses the default MTU size for the underlying medium.

You can specify a different MTU size for the configured link from 0 to 65535. IPv6 considers this value only if it is less than the default MTU of the underlying medium.

Enter 0 if you want IPv6 to use the default MTU of the underlying medium.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Link MTU** parameter. Click on **Help** or see the parameter description on page A-5.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Size of the Forwarding Table

By default, IPv6 allows a maximum of 128 entries in the interface forwarding table (also called the cache) at one time. There is a forwarding table for each interface.

You can use the following Site Manager procedure to configure a forwarding table for 0 to 20480 entries.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Cache Size** parameter. Click on **Help** or see the parameter description on page A-5.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring IPv6 on the Circuitless Interface

If you want to configure IPv6 on the circuitless interface, you must set the circuit number to a value greater than 1023.

You can use the following Site Manager procedure to specify a slot or indicate acceptable slots for the circuitless interface.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Slot Mask** parameter. Click on **Help** or see the parameter description on page A-5.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Enabling and Disabling Redirect Messages

By default, IPv6 sends Internet Control Message Protocol (ICMP) redirect messages on this interface.

You can use the following Site Manager procedure to disable and reenable redirect messages on the IPv6 interface.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Redirect On/Off** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring ICMP Error Messages

By default, IPv6 is allowed to transmit up to 100 ICMP error messages per second on this interface.

You can use the following Site Manager procedure to supply a different maximum number.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Max ICMP Messages** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Enabling and Disabling TR End Station Support

By default, IPv6 does not provide source routing support for a token ring network.

If the interface is connected to a token ring network, you can use the following Site Manager procedure to enable TR end station support.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **TR End Station** parameter. Click on **Help** or see the parameter description on page A-6.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying an SMDS Group Address

You can use the following Site Manager procedure to provide a switched multimegabit data service (SMDS) group address for this interface.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **SMDS Group Address** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying Frame Relay Broadcast DLCI

You can use the following Site Manager procedure to supply a frame relay broadcast data link connection identifier (DLCI).

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Frame Relay Broadcast DLCI** parameter. Click on **Help** or see the parameter description on page A-7.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying Frame Relay Multicast DLCI

You can use the following Site Manager procedure to supply frame relay multicast DLCI numbers 1 and 2.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the following parameters: • **Frame Relay Multicast DLCI #1** • **Frame Relay Multicast DLCI #2** Click on **Help** or see the parameter descriptions beginning on page A-7.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring a Tunnel on the Interface

For an overview of tunnels and information about the types of tunnels you can configure on an IPv6 interface, see “Tunnels” on page 1-21.

To configure a tunnel on this interface,

1. **Configure the IPv6 interface as a tunnel end point.**
2. **Specify the type of type of tunnel you want to configure.**
3. **Supply the local and remote end point addresses required for the type of tunnel you are configuring.**

These operations are described under the following topics:

Topic	Page
Configuring an IPv6 Interface as a Tunnel End Point	3-24
Specifying a Tunnel Type	3-25
Specifying a Local IPv4 Address	3-27
Specifying a Remote IPv4 Address	3-28
Specifying a Local IPv6 Index	3-29
Specifying a Remote IPv6 Address	3-30

Configuring an IPv6 Interface as a Tunnel End Point

To indicate that the interface is the end point of a tunnel, use the following Site Manager procedure to enter a circuit number of 0.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Circuit Name** parameter with the value 0.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Tunnel Type

For information about IPv6 and IPv4 tunnel types, see “Tunnels” on page 1-21.

IPv6 supports the following types of tunnels:

- *IPv4 static tunnel*. If you specify an IPv4 static tunnel, you must supply an IPv4 address for the local and remote end point.
- *IPv4 automatic tunnel.* If you specify an IPv4 automatic tunnel, you must supply an IPv4 address for the local end point.
- *IPv4 semiautomatic tunnel.* If you specify an IPv4 semiautomatic tunnel, you must supply an IPv4 address for the local and remote end points.
- *IPv6 static tunnel.* If you specify an IPv6 static tunnel, you must supply an IPv6 index number for the local end point and supply an IPv6 address for remote end point.
- *IPv6 automatic tunnel.* If you specify an IPv6 automatic tunnel, you must supply an IPv6 address for the local end point.
- *IPv6 semiautomatic tunnel.* If you specify an IPv6 semiautomatic tunnel, you must supply an IPv6 index number for the local end point and supply an IPv6 address for the remote end point.

You can use the following Site Manager procedure to specify the type of tunnel you want you want to configure on the interface.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Tunnel Protocol Type** parameter. Click on **Help** or see the parameter description on page A-8.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Local IPv4 Address

If you are configuring an IPv4 static tunnel, an IPv4 automatic tunnel, or an IPv4 semiautomatic tunnel, you must supply the IP address of the local IPv4 end point.

This address becomes the source address in the encapsulating IPv4 header.

You can use the following Site Manager procedure to specify a local IPv4 address.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Tunnel IPv4 Local Address** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Remote IPv4 Address

If you are configuring an IPv4 static tunnel or an IPv4 semiautomatic tunnel, you must supply a remote IPv4 address.

For a static tunnel and a semiautomatic tunnel, this address becomes the destination address in the encapsulating IPv4 header.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Tunnel IPv4 Remote Address** parameter. Click on **Help** or see the parameter description on page A-9.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Local IPv6 Index

If you are configuring an IPv6 static tunnel, an IPv6 automatic tunnel, or an IPv6 semiautomatic tunnel, you must supply the IPv6 index of the local IPv6 end point.

This index is used to create the source address in the encapsulating IPv6 header.

You can use the following Site Manager procedure to supply a local IPv6 index.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **IPv6 Local Index** parameter. Click on **Help** or see the parameter description on page A-10.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Remote IPv6 Address

If you are configuring an IPv6 static tunnel or an IPv6 semiautomatic tunnel, you must supply a remote IPv6 address.

For a static tunnel and a semiautomatic tunnel, this address becomes the destination address in the encapsulating IPv6 header.

You can use the following Site Manager procedure to supply a remote IPv6 address.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **Edit IPv6 Interfaces**.	The IPv6 Interfaces window opens.
4. Click on the interface you want to edit.	Site Manager displays the parameter values for that interface.
5. Set the **Tunnel IPv6 Remote Address** parameter. Click on **Help** or see the parameter description on page A-10.	
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring an IPv6 Address Prefix

An IPv6 address consists of an interface ID and an address prefix. For information about IPv6 addresses, see Chapter 1.

You configure an IPv6 address prefix by setting parameters as described under the following topics:

Section	Page
Associating a Prefix with an interface ID	3-32
Enabling and Disabling Use of the Prefix	3-33
Supplying an Address Prefix	3-34
Specifying the Length of the Prefix	3-35
Specifying a Routing Preference	3-36
Specifying a Cost	3-37
Configuring the Prefix for On-Link Determination	3-38
Enabling Autonomous Address Configuration	3-39
Supplying a Preferred Lifetime Value	3-40
Supplying a Valid Lifetime Value	3-41

Associating a Prefix with an interface ID

You can use following Site Manager procedure to add an address prefix to an interface ID to create a complete IPv6 address.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Click on **Add**.	The Values Selection window opens.
5. Choose the IPv6 index of the interface to which you want to add the prefix.	The IPv6 Prefixes window reopens.
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Enabling and Disabling Use of the Prefix

By default, an address prefix you configure is enabled for use.

You can use the following Site Manager procedure to disable and reenable the prefix.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-11.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying an Address Prefix

You can use the following Site Manager procedure to supply the address prefix.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Interface Prefix** parameter. Click on **Help** or see the parameter description on page A-11.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Length of the Prefix

An address prefix can be 3 to 128 bits long.

You can use the following Site Manager procedure to specify the length of this address prefix.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Prefix Length** parameter. Click on **Help** or see the parameter description on page A-11.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Routing Preference

The default routing preference value is 15 (most preferred).

You can use the following Site Manager procedure to specify a routing preference value from 1 to 15.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Routing Preference** parameter. Click on **Help** or see the parameter description on page A-12.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Cost

The default cost of an address prefix is 1.

You can use the following Site Manager procedure to specify a cost from 1 to 15.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Prefix Cost** parameter. Click on **Help** or see the parameter description on page A-12.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring the Prefix for On-Link Determination

By default, an address prefix can be used for on-link determination.

You can use the following Site Manager procedure to disable and reenable this feature.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **On Link Flag** parameter. Click on **Help** or see the parameter description on page A-12.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Enabling Autonomous Address Configuration

By default, this prefix can be used for autonomous address configuration -- that is, to form a local interface address.

You can use the following Site Manager procedure to disable and reenable this feature.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Autonomous Prefix Flag** parameter. Click on **Help** or see the parameter description on page A-13.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying a Preferred Lifetime Value

The referred lifetime value indicates the length of time in seconds (relative to the time the router advertisement is sent) that this prefix will remain preferred -- that is, the time until deprecation.

The default lifetime, 0xffffffff (-1), represents infinity.

IPv6 places this value in the preferred lifetime field in the prefix information option of a router advertisement.

When the preferred lifetime expires, the address generated from a deprecated prefix should no longer be used as a source address in new communications. However, packets received on such an interface are processed as expected.

You can use the following Site Manager procedure to supply a preferred lifetime value.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Relative Preferred Lifetime** parameter. Click on **Help** or see the parameter description on page A-13.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying a Valid Lifetime Value

The valid lifetime value indicates the length of time in seconds (relative to the time the router advertisement is sent) that this prefix remains valid.

The default lifetime, 0xffffffff (-1), represents infinity.

IPv6 places this value in the valid lifetime field in the prefix information option of router advertisements.

The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

You can use the following Site Manager procedure to supply a valid lifetime value.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Prefixes**.	The IPv6 Prefixes window opens.
4. Set the **Relative Valid Lifetime** parameter. Click on **Help** or see the parameter description on page A-14.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Customizing IPv6 Neighbor Discovery

For an overview, see “Neighbor Discovery” on page 1-27.

When you configure IPv6 on an interface, neighbor discovery is automatically added to the interface. You customize neighbor discovery by modifying neighbor discovery parameters as described under the following topics:

Topic	Page
Enabling and Disabling Neighbor Discovery	3-43
Controlling Router Advertisements	3-44
Controlling Address Autoconfiguration	3-45
Controlling Nonaddress Autoconfiguration	3-46
Specifying a Neighbor Reachability Time	3-47
Specifying a Retransmission Time For Neighbor Solicitations	3-48
Specifying a Maximum Hop Limit for ND Advertisements	3-49
Specifying a Minimum Time for Unsolicited Advertisements	3-50
Specifying a Maximum Time for Unsolicited Advertisements	3-51
Specifying a Lifetime for the Default Router	3-52
Configuring Address Duplication Detection	3-53

Enabling and Disabling Neighbor Discovery

By default, neighbor discovery is enabled on the interface.

You can use the following Site Manager procedure to change the state of neighbor discovery as required.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-14.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Controlling Router Advertisements

An IPv6 router receives ND solicitations messages from hosts on local networks. The router responds by returning a unicast route advertisement message.

In addition to these responses, an IPv6 router can also send router advertisements periodically on the interface to local multicast groups, whether or not they receive solicitations.

You can use the following Site Manager procedure to control whether or not IPv6 sends periodic route advertisements on the interface.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Router Advertisement** parameter. Click on **Help** or see the parameter description on page A-14.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Controlling Address Autoconfiguration

Using the router advertisement that it sends in response to a solicitation message from a host, an IPv6 router can control whether the host uses stateful or stateless autoconfiguration.

By default, the router instructs the host to use stateless autoconfiguration.

The following Site Manager procedure lets you configure IPv6 to instruct hosts to use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Managed Address Configuration** parameter. Click on **Help** or see the parameter description on page A-15.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Controlling Nonaddress Autoconfiguration

Turn the Managed Non-Address flag on if you want hosts to use the administered (stateful) protocol for autoconfiguration of nonaddress information.

You can use the following Site Manager procedure to set the nonaddress flag as required.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Managed Non-Address** parameter. Click on **Help** or see the parameter description on page A-15.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Neighbor Reachability Time

The neighbor reachability time is the number of milliseconds (ms) that a node assumes a neighbor is reachable after having received a reachability confirmation. By default, the router does not specify a reachability time (indicated by a value of 0).

You can use the following Site Manager procedure to specify a neighbor reachability time.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Reachable Time** parameter. Click on **Help** or see the parameter description on page A-15.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Retransmission Time For Neighbor Solicitations

The retransmission time for neighbor solicitations is the number of milliseconds between retransmitted neighbor solicitation messages.

The default value is 0, indicating that the retransmission time is unspecified (by this router).

You can use the following Site Manager procedure to specify a retransmission time for neighbor solicitations.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Retransmission Time** parameter. Click on **Help** or see the parameter description on page A-16.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Maximum Hop Limit for ND Advertisements

The default maximum hop limit for ND advertisements is 64 hops.

You can use the following Site Manager procedure to specify a maximum hop limit from 0 to 255 hops**.**

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Maximum Hop Limit** parameter. Click on **Help** or see the parameter description on page A-16.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Minimum Time for Unsolicited Advertisements

The minimum time for unsolicited advertisements is the minimum rate (in seconds) at which the router can send unsolicited multicast router advertisements on this interface.

The default minimum time is 200 seconds. The allowable range is 3 to 1350 seconds.

You can use the following Site Manager procedure to specify a minimum time for unsolicited advertisements.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Minimum Multicast** parameter. Click on **Help** or see the parameter description on page A-16.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Maximum Time for Unsolicited Advertisements

The maximum time for unsolicited advertisements is the maximum rate (in seconds) at which the router can send unsolicited multicast router advertisements on this interface.

The default maximum time is 600 seconds. The allowable range is 4 to 1800 seconds.

You can use the following Site Manager procedure to set the maximum time for unsolicited advertisements.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Maximum Multicast** parameter. Click on **Help** or see the parameter description on page A-17.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Lifetime for the Default Router

By default, the default router has a lifetime of 1800 seconds. The allowable lifetime range is 0 to 9000 seconds.

You can use the following Site Manager procedure to specify a lifetime for the default router.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Default Lifetime** parameter. Click on **Help** or see the parameter description on page A-17.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring Address Duplication Detection

By default, the router sends a single neighbor solicitation message (with no follow-up retransmission) while performing duplicate address detection on a tentative address.

You can use the following Site Manager procedure to supply a value from 0 to 10, where 0 indicates that no duplicate address detection needs to be performed.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Neighbor Discovery**.	The IPv6 Neighbor Discovery window opens.
4. Set the **Duplicate Address Detection** parameter. Click on **Help** or see the parameter description on page A-17.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Defining an IPv6 Adjacent Node

An adjacent node is a device attached to a local network. You define an adjacent node by supplying information and setting values as described under the following topics:

Topic	Page
Enabling and Disabling the Adjacent Node Definition	3-55
Supplying the Physical Address of the Adjacent Node	3-56
Specifying the Link Layer Encapsulation Type	3-57
Specifying a Route Preference Value	3-58
Specifying the Cost	3-59
Supplying the WAN Address of the Adjacent Node	3-60

Enabling and Disabling the Adjacent Node Definition

By default, the adjacent node definition that you are creating is enabled on the router.

You can use the following Site Manager procedure to disable and reenable the adjacent node definition as required.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Adjacent Nodes**.	The IPv6 Adjacent Nodes window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-18.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying the Physical Address of the Adjacent Node

For a frame relay PVC, the physical address of the adjacent node is a 32-bit DLCI. For an ATM PVC this address is a 32-bit VCID which has circuit VCI in its most significant 20 bits and VPI in 12 least significant bits.

You can use the following Site Manager procedure to supply the physical address of this adjacent node.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Adjacent Nodes**.	The IPv6 Adjacent Nodes window opens.
4. Set the **Physical Address** parameter. Click on **Help** or see the parameter description on page A-18.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Link Layer Encapsulation Type

By default, the link layer encapsulation type defined for the adjacent node is "other."

The link layer encapsulation type used by the adjacent node depends on the type of network on which the node is located. You can use the following Site Manager procedure to specify SNAP encapsulation for a IEEE 802.2 network, PDN encapsulation for X.25 PDN, and WAN for frame relay SVC and ATM SVC.

Specify Subnetwork Access Protocol (SNAP) encapsulation only if IEEE 802.2 encapsulation is to be used over CSMA/CD or DS1 links.

You can use the following Site Manager procedure to specify a link layer encapsulation type.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Adjacent Nodes**.	The IPv6 Adjacent Nodes window opens.
4. Set the **Link Layer Encapsulation** parameter. Click on **Help** or see the parameter description on page A-18.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Route Preference Value

By default, this definition has a preference value of 15 (most preferred).

You can use the following Site Manager procedure to specify a preference from 0 to 15.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Adjacent Nodes**.	The IPv6 Adjacent Nodes window opens.
4. Set the **Routing Preference** parameter. Click on **Help** or see the parameter description on page A-19.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Cost

By default, this adjacent node definition has a cost of 1.

The cost value you specify is used as the RIP metric.

You can use the following Site Manager procedure to specify a cost value from 1 to 15.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Adjacent Nodes**.	The IPv6 Adjacent Nodes window opens.
4. Set the **Cost** parameter. Click on **Help** or see the parameter description on page A-19.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying the WAN Address of the Adjacent Node

IPv6 uses a WAN address (for example, an X.121 or E.164 address) to establish an SVC to the adjacent host. For an X.25 PVC, this parameter contains the logical channel number (LCN) of the permanent virtual circuit (PVC) encoded as an X.121 address up to 4 octets in length.

You can use the following Site Manager procedure to specify the WAN address of the adjacent node.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Adjacent Nodes**.	The IPv6 Adjacent Nodes window opens.
4. Set the **X.121 Address** parameter. Click on **Help** or see the parameter description on page A-19.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring an IPv6 Static Route

A static route is a manually configured route that specifies the next hop a datagram must follow to reach the destination expressed in the destination address.

You configure an IPv6 static route by setting parameters as described under the following topics:

Topic	Page
Associating the Static Route with an Interface	3-61
Enabling and Disabling the Static Route	3-62
Supplying the Destination IPv6 Address Prefix	3-63
Specifying the Prefix Length	3-64
Supplying the IPv6 Next-Hop Address	3-65
Specifying a Route Preference Value	3-66
Specifying the Cost	3-67

Associating the Static Route with an Interface

You can use the following Site Manager procedure to associate the static route with an interface.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Static Routes**.	The IPv6 Static Routes window opens.
4. Click on **Add**.	The Values Selection window opens.
5. Choose the IPv6 index of the interface to which you want to add the prefix.	The IPv6 Prefixes window reopens.
6. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Enabling and Disabling the Static Route

By default, the static route you configure is enabled.

You can use the following Site Manager procedure to disable and reenable the static route.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Static Routes**.	The IPv6 Static Routes window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-20.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying the Destination IPv6 Address Prefix

You can use the following Site Manager procedure to specify the destination address prefix for the static route.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Static Routes**.	The IPv6 Static Routes window opens.
4. Set the **Prefix** parameter. Click on **Help** or see the parameter description on page A-20.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Prefix Length

You can use the following Site Manager procedure to specify the length (in bits) of the destination address prefix.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Static Routes**.	The IPv6 Static Routes window opens.
4. Set the **Prefix Length** parameter. Click on **Help** or see the parameter description on page A-20.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying the IPv6 Next-Hop Address

You can use the following Site Manager procedure to supply the IPv6 address of next-hop node.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Static Routes**.	The IPv6 Static Routes window opens.
4. Set the **Next Hop Address** parameter. Click on **Help** or see the parameter description on page A-21.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Route Preference Value

By default, the static route has a preference value of 15 (most preferred).

You can use the following Site Manager procedure to specify a preference value from 0 to 15.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Static Routes**.	The IPv6 Static Routes window opens.
4. Set the **Route Preference** parameter. Click on **Help** or see the parameter description on page A-21.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Cost

By default, the static route has a cost of 1.

You can use the following Site Manager procedure to specify a cost from 0 to 15.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List Static Routes**.	The IPv6 Static Routes window opens.
4. Set the **Cost** parameter. Click on **Help** or see the parameter description on page A-21.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring a Static Default Route

A default route entry in the routing table has a destination address of 0. If the router is unable to match the destination address on a received packet with a destination address in the routing table, the router uses the default route.

You can use Site Manager to configure a static default route.

1. **Add the static route to the IP interface that you want to use for the default route.**

   See “Configuring an IPv6 Static Route” on page 3-61.

2. **In the List Static Routes window, set the Prefix Length parameter to 0.**

Configuring a Black Hole

A router that advertises an aggregate route uses a mechanism called a black hole to discard packets that match the aggregate address but that do not match any of the explicit routes.

You can use Site Manager to configure a black hole.

1. **Configure a static route for the destination address you want to discard.**
2. **In the List Static Routes window, click on Black Hole.**

Chapter 4
Configuring RIPv6

You configure RIPv6 by setting parameters as described under the following topics:

Topic	Page
Enabling and Disabling RIP	4-2
Supplying RIP Updates	4-3
Receiving RIP Updates	4-4
Supplying a Default Route	4-5
Listening for a Default Route	4-6
Specifying the Update Mode	4-7
Specifying an Interval for Update Broadcasts	4-8
Specifying a Timeout Period for an Unreachable Network	4-9
Specifying a Hold Down Time	4-10
Sending Triggered Updates	4-11
Specifying the RIPv6 Diameter	4-12
Configuring RIPv6 Policies	4-13

Enabling and Disabling RIP

When you add RIPv6 to an IPv6 interface, RIPv6 is enabled by default.

You can use the following Site Manager procedure to disable and reenable IPv6 on the interface as required.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Enable** parameter. Click on **Help** or see the parameter description on page A-22.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying RIP Updates

By default, RIP supplies RIP updates to neighboring networks on each interface.

You can use the following Site Manager procedure to disable and reenable updates on this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **RIP Supply** parameter. Click on **Help** or see the parameter description on page A-22.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Receiving RIP Updates

By default, RIPv6 listens for routing updates on every interface on which it is enabled.

If you choose Enable, RIPv6 listens for updates on this interface and adds received routing information to its internal routing table. If you choose Enable, a configured policy can still prohibit the interface from updating its internal routing tables.

If you choose Disable, RIPv6 ignores updates received on this interface from neighboring routers. RIPv6 does not add received routing information to its internal routing table.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **RIP Listen** parameter. Click on **Help** or see the parameter description on page A-22.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Supplying a Default Route

When the routing table does not contain the route to a particular destination address, the router looks for a default route to the destination. Like any other route in the routing table, the default route can be acquired dynamically (by means of a routing protocol) or entered statically (by you).

This parameter is independent of the RIP Supply parameter. A configured policy can override the parameter.

By default, RIP does not supply a default route.

If you choose Enable, RIP advertises the default route if it is present in the routing table -- that is, if you have statically included a default route in the table or if the router has learned the default route dynamically.

If you choose Generate, RIP advertises a default route whether or not a default route is present in the routing table. (This parameter does not cause RIP to create a routing table entry for a default route; the route will not be visible in the routing table.)

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Default Route Supply** parameter. Click on **Help** or see the parameter description on page A-23.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Listening for a Default Route

By default, RIPv6 ignores inbound advertisements of a default route on the interfaces where it is configured. You can use the BCC or Site Manager to configure RIPv6 to listen for a default route.

If you choose Enable, RIPv6 listens for a default route on this interface and adds the default route information to its internal routing table. Note that you must also enable RIP Listen on this interface. A configured policy can override this setting.

If you choose Disable, RIPv6 does not listen for a default route on this interface and does not add the default route information to its internal routing table.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Default Route Listen** parameter. Click on **Help** or see the parameter description on page A-23.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the Update Mode

RIPv6 can issue routing updates on this interface in the following modes:

- Poisoned reverse (the default)
- Split horizon
- Actual cost

If you enable poisoned reverse mode on this interface, RIPv6 advertises routes to the adjacent network from which it has learned the routes. In RIP updates, RIPv6 uses a hop count of RIP Network Diameter plus one, thus declaring the destination unreachable. Poisoned reverse can speed up the convergence of the network routing tables.

If you enable split horizon mode on this interface, RIPv6 omits routes learned from a neighbor in RIP updates subsequently sent to that neighbor.

If you enable actual cost mode on this interface, RIPv6 advertises routes with the learned cost. This is useful on a frame relay interface that has virtual connections (VCs) to different routers that are part of the same logical IP subnet.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Poison** parameter. Click on **Help** or see the parameter description on page A-24.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying an Interval for Update Broadcasts

By default, RIP generates a full update every 30 seconds on each interface configured with RIP.

If you have enabled dial-optimized routing on this interface, the default is 1 hour.

You can use the following Site Manager procedure to specify a different update interval for the interface from 5 to 86,400 seconds. For dial-optimized routing the range is 3600 seconds (1 hour) to 1,209,600 seconds (2 weeks).

Enter a value in 5-second increments.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Broadcast Time** parameter. Click on **Help** or see the parameter description on page A-24.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Timeout Period for an Unreachable Network

By default, RIP waits 90 seconds for an update from a network before it considers that network to be unreachable.

If you have enabled dial-optimized routing on this interface, the default is 3 hours.

You can specify a timeout period from 15 seconds to 259,200 seconds (72 hours). For dial-optimized routing, the maximum value is 3,628,800 seconds (6 weeks).

We recommend a timeout value of the broadcast time multiplied by 3. Enter a time in 5-second increments.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Timeout Timer** parameter. Click on **Help** or see the parameter description on page A-25.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying a Hold Down Time

Once RIP has determined that a network is unreachable, RIP continues to advertise a route to that network for a default holddown period of 90 seconds.

If you have enabled dial-optimized routing on this interface, the default is 3 hours.

We recommend a timeout value of the broadcast time multiplied by 3. Enter a time in 5-second increments. This parameter affects how long a route remains in the routing table after the route has become unusable. To guarantee the holddown time for each interface, RIP uses the largest holddown value as the amount of time to keep the route in the routing table. Please note that if a route to a destination becomes unusable, the holddown value will not affect the router's ability to learn new routes to the same destination.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Hold Down Timer** parameter. Click on **Help** or see the parameter description on page A-25.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Sending Triggered Updates

RIP generates full routing updates at regular intervals. You can also configure RIP to generate an update on a specified interface each time it recalculates a route's metric. Such an update is called a *triggered update*. A triggered update contains only the routes that have changed. (RIP also sends full updates at regular intervals on interfaces configured for triggered updating.)

If you enable triggered updates, RIP will generate triggered updates with a maximum frequency of one every 5 seconds. The route will include all changes that occurred in the last 5 seconds. This enforced interval prevents RIP from monopolizing CPU resources during periods of instability.

By default, triggered updates are disabled on all interfaces configured for RIP.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **Triggered Updates** parameter. Click on **Help** or see the parameter description on page A-26.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Specifying the RIPv6 Diameter

The RIP diameter is a hop count that RIPv6 uses to denote infinity.

You must set this parameter so that none of the interface cost, static cost, or route filter cost parameters exceed the RIP diameter. We recommend that you accept the default RIP diameter value of 15.

You can use the following Site Manager procedure to perform this operation.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **List RIP Interfaces**.	The IPv6 RIP Interfaces window opens.
4. Set the **RIP Diameter** parameter. Click on **Help** or see the parameter description on page A-26.	
5. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring RIPv6 Policies

RIPv6 policies allow you to control the flow of routing information in and out of the routing table.

- A policy that controls the routing information that is considered for inclusion in the IPv6 routing table is called an *accept policy.*
- A policy that controls the routing information that RIPv6 advertises is called an *announce policy.*

RIPv6 accept and announce policies are described under the following topics:

Topic	Page
Configuring a RIPv6 Accept Policy	4-14
Configuring a RIPv6 Announce Policy	4-16

Configuring a RIPv6 Accept Policy

A RIPv6 accept policy governs the addition of new routes to the routing tables. Accept policy parameters fall into the following categories:

- Name. You use the Accept Name parameter to supply a unique name for the RIPv6 accept policy.
- State. You use the Enable parameter to enable and disable the RIPv6 accept policy.
- Match. You use the Prefixes, Preference, Precedence, Gateway, and Interface parameters to specify criteria. If a received update matches the criteria you specify, IPv6 takes the action you specify.
- Action. You use the Action, Injection, and Log parameters to specify the operations that RIPv6 performs on a received update that matches the criteria you have specified for the policy.

You can use the following Site Manager procedure to configure a RIPv6 accept policy.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **RIPv6**.	The RIPv6 window opens.
4. Choose **Policies.**	
5. Choose **Accept**.	The RIPv6 Accept Policies window opens.
6. Set the following parameters: • **Accept Enable** • **Accept Name** • **Accept Prefixes** • **Accept Action** • **Accept Preference** • **Accept Precedence** • **Accept Inject** • **Accept Gateway** • **Accept Interface** • **Accept Log** Click on **Help** or see the parameter descriptions beginning on page A-26.	
7. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Configuring a RIPv6 Announce Policy

An announce policy governs the advertisement of routing information. When preparing a routing advertisement, RIPv6 consults its announce policies to determine whether or not to advertise the route. Announce policy parameters fall into the following categories:

- Name. You use the Announce Name parameter to supply a unique name for the RIPv6 announce policy.
- State. You use the Enable parameter to enable and disable the RIPv6 announce policy.
- Match. You use the Prefixes, Precedence, Route Source, External Route Source Gateway, Interface, and Metric parameters to specify update characteristics. If a received update matches the criteria you specify, IPv6 takes the action you specify.
- Action. You use the Action and Advertise parameters to specify the operations that RIPv6 performs on an outbound update that matches the criteria you have specified for the policy.

You can use the following Site Manager procedure to configure a RIPv6 announce policy.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols**.	The Protocols menu opens.
2. Choose **IPv6**.	The IPv6 menu opens.
3. Choose **RIPv6**.	The RIPv6 window opens.
4. Choose **Policies.**	
5. Choose **Announce**.	The RIPv6 Announce Policies window opens.
6. Set the following parameters: • **Announce Enable** • **Announce Name** • **Announce Prefixes** • **Announce Action** • **Announce Precedence** • **Announce Route Source** • **Announce External Route Source** • **Announce Advertise** • **Announce RIP Gateway** • **Announce Interface** • **Announce RIP Metric** Click on **Help** or see the parameter descriptions beginning on page A-31.	
7. Click on **Apply**, and then click on **Done**.	Site Manager returns you to the Configuration Manager window.

Appendix A
Site Manager Parameters for IPv6

IPv6 Global Parameters

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IPv6 > IPv6 Global
Default:	Enable
Options:	Enable | Disable
Function:	Enables and disables IPv6 globally.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.1.2

Parameter:	**Forwarding**
Path:	Configuration Manager > Protocols > IPv6 > IPv6 Global
Default:	Forwarding
Options:	Forwarding | Notforwarding
Function:	Specifies whether this entity is acting as an IPv6 router with respect to the forwarding of datagrams received by, but not addressed to, this entity. IPv6 routers forward datagrams. IPv6 hosts do not (except datagrams source-routed via the host).
Instructions:	For some managed nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a “badValue” response if a management station attempts to change this object to an inappropriate value.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.1.4

Parameter: Default Hop

Path: Configuration Manager > Protocols > IPv6 > IPv6 Global
Default: 64
Options: 0 to 255
Function: Supplies the default value that IPv6 inserts into the hop limit field of the IPv6 header of datagrams originated at this entity whenever a hop-limit value is not supplied by the transport layer protocol.
Instructions: Accept the default value or supply a different value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.1.5

Parameter: Minimum Link MTU

Path: Configuration Manager > Protocols > IPv6 > IPv6 Global
Default: 576
Options: 296 to 65535
Function: Indicates the minimum link MTU size that is assumed for every link in the IPv6 internet.
Instructions: By changing this parameter, you can control the maximum size of packets that can be generated by this router if MTU path discovery is disabled.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.1.6

Parameter: MTU Discovery

Path: Configuration Manager > Protocols > IPv6 > IPv6 Global
Default: Enable
Options: Enable | Disable
Function: Enables and disables path MTU discovery support for self-originated traffic.
Instructions: Disable this feature if you want to use the Minimum Link MTU parameter to control the maximum size of self-generated packets.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.1.7

Parameter:	**MTU Timeouts**
Path:	Configuration Manager > Protocols > IPv6 > IPv6 Global
Default:	10 minutes
Options:	0 (no MTU timeout) or 1 to 71582788
Function:	Timeout period for discovered path MTU values in minutes.
Instructions:	To disable MTU timeouts, set this parameter to 0.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.1.8

IPV6 Interface Parameters

Parameter:	**Enable**
Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Enables and disables this IPv6 interface.
Instructions:	Set this parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.2

Parameter:	**Interface Description**
Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	None
Options:	Text string of 0 to 255 characters
Function:	Supplies an optional text string containing a description of the interface.
Instructions:	Use this parameter to supply an optional description of the interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.5

Parameter: Interface Token

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces

Default: See Instructions.

Options: Text string of 0 to 6 characters

Function: Supplies an identifier (an interface token) for this interface that is unique on the link to which this interface is attached. The interface token is combined with an address prefix to form an interface address.

Instructions: If you do not configure a token, the interface token is autoconfigured according to the rules of the link type to which this interface is attached.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.7

Parameter: Circuit Name

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces

Default: The name of the circuit on which you have configured the IPv6 interface

Options: A valid circuit name

Function: Identifies the circuit that the interface runs over.

Zero indicates that this is a tunnel end point. In IPv6 tunneling, IPv6 packets are encapsulated and transmitted by another network layer protocol or another instance of the IPv6 protocol. A value greater than 1023 indicates that the interface is the circuitless interface.

Instructions: Supply a value that identifies this circuit.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.6

Parameter: Link Layer Address

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces

Default: None

Options: A valid link layer address

Function: Specifies the link layer address for this IPv6 interface

Instructions: Supply a link layer address.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.11

Parameter: Link MTU

Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	0
Options:	0 to 65535
Function:	Specifies an MTU size for the configured link. IPv6 considers this value only if it is less than the default MTU of the underlying medium. A value of 0 indicates that the default MTU of the underlying medium is to be used.
Instructions:	Use the default (0) or specify a value that is less than the MTU of the underlying medium.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.13

Parameter: Cache Size

Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	128 entries
Options:	0 to 20480 entries
Function:	Specifies the maximum number of entries allowed in the forwarding table at one time. There is a forwarding table, or cache, for each interface.
Instructions:	Enter 0 if you do not want IPv6 to configure a forwarding table on this interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.14

Parameter: Slot Mask

Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	4294705152
Options:	Slot 1 to 14
Function:	Specifies which slots a circuitless interface is eligible to run on.
Instructions:	You must set the circuit number to a value greater than 1023. See the Circuit Name parameter.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.15

Parameter: Redirect On/Off

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default: On
Options: On │ Off
Function: Specifies whether IPv6 sends ICMP redirect messages on this interface.
Instructions: Set this parameter to Off if you want to disable redirects on this IPv6 interface.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.19

Parameter: Max ICMP Messages

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default: 100 messages
Options: An integer
Function: Specifies the maximum number of ICMP error messages that IPv6 is allowed to transmit on this interface within a 1-second interval.
Instructions: Use the default or specify another value.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.20

Parameter: TR End Station

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default: Off
Options: On │ Off
Function: Turns on source routing support for a token ring network.
Instructions: This parameter applies only if the interface is connected to a token ring network.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.21

Parameter: **SMDS Group Address**

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default: None
Options: A valid SMDS group address
Function: Specifies an SMDS group address for the interface.
Instructions: Supply the required address.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.22

Parameter: **Frame Relay Broadcast DLCI**

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default: None
Options: A valid frame relay broadcast DLCI
Function: Specifies a frame relay broadcast DLCI for this IPv6 interface.
Instructions: Supply the required address.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.23

Parameter: **Frame Relay Multicast DLCI #1**

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default: None
Options: A valid frame relay multicast DLCI
Function: Specifies a frame relay multicast DLCI #1 for this IPv6 interface.
Instructions: Supply the required address.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.24

Parameter: **Frame Relay Multicast DLCI #2**

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default: None
Options: A valid frame relay multicast DLCI
Function: Specifies a frame relay multicast DLCI #2 for this IPv6 interface.
Instructions: Supply the required address.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.25

Parameter: Tunnel Protocol Type

Path: Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces

Default: ip4st

Options: ip4st │ IPv6st │ ip4sa │ IPv6sa │ ip4au │ IPv6au

Function: If the Circuit Name parameter is set to 0, this parameter specifies the tunnel protocol type:

ip4st - IPv6-in-IPv4 static tunnel
IPv6st - IPv6-in-IPv6 static tunnel
ip4sa - IPv6-in-IPv4 semiautomatic tunnel
IPv6sa - IPv6-in-IPv6 semiautomatic tunnel
ip4au - IPv6-in-IPv4 automatic tunnel
IPv6au - IPv6-in-IPv6 automatic tunnel

A static tunnel is a tunnel with defined (static) local and remote end points. You define a tunnel end point by assigning an address. Static tunnels are also called configured tunnels.

An automatic tunnel is a tunnel that does have a predefined remote address. The destination address of the encapsulating header is derived from the destination address of the encapsulated packet.

A semiautomatic tunnel acts as a static tunnel for outgoing traffic and as an automatic (multipoint-to-point) tunnel for incoming traffic. Both local and remote end points must be configured.

Instructions: To specify a protocol type for the tunnel, you must set the Circuit Name parameter to 0.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.26

Parameter: Tunnel IPv4 Local Address

Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	None
Options:	An IPv4 address
Function:	If the Circuit Name parameter is set to 0 and the Tunnel Protocol Type parameter is set to ip4st or ip4sa, this parameter contains the local IPv4 address of the tunnel connected to this interface.
Instructions:	Make sure the Circuit Name parameter and the Tunnel Protocol Type parameter are set appropriately.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.27

Parameter: Tunnel IPv4 Remote Address

Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	None
Options:	An IPv4 address
Function:	If the Circuit Name parameter is set to 0 and the Tunnel Protocol Type parameter is ip4st or ip4sa, this parameter contains the remote IPv4 address of this interface's tunnel. If this address is 0.0.0.0, this is an interface to an automatic tunnel -- that is, the destination address of the encapsulating header is derived from the destination address of the encapsulated packet.
Instructions:	Make sure the Circuit Name parameter and the Tunnel Protocol Type parameter are set appropriately.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.28

Parameter: IPv6 Local Index

Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	None
Options:	An IPv6 interface index value
Function:	If the Circuit Name parameter is set to 0 and the Tunnel Protocol Type parameter is set to IPv6st or IPv6sa, this parameter contains the IPv6 interface index of the local end of this interface's tunnel.
Instructions:	Make sure the Circuit Name parameter and the Tunnel Protocol Type parameter are set appropriately.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.29

Parameter: Tunnel IPv6 Remote Address

Path:	Configuration Manager > Protocols > IPv6 > Edit IPv6 Interfaces
Default:	None
Options:	An IPv6 address
Function:	If the Circuit Name parameter is set to 0 and the Tunnel Protocol Type parameter is set to ipv6st or IPv6sa, this parameter contains the remote IPv6 address of the tunnel connected to this interface. If this address is unspecified (::0), this is an interface to an automatic tunnel -- that is, the destination address of the encapsulating header is derived from the destination address of the encapsulated packet.
Instructions:	Make sure the Circuit Name parameter and the Tunnel Protocol Type parameter are set appropriately.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.2.1.30

IPv6 Prefix Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IPv6 > List Prefixes
Default: Enable
Options: Enable | Disable
Function: Enables and disables the use of this prefix.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.2

Parameter: Interface Prefix

Path: Configuration Manager > Protocols > IPv6 > List Prefixes
Default: None
Options: An IPv6 address prefix
Function: Supplies the address prefix associated with the IPv6 address of this interface.
Instructions: Supply an IPv6 address prefix. Use the Prefix Length parameter to specify its length.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.5

Parameter: Prefix Length

Path: Configuration Manager > Protocols > IPv6 > List Prefixes
Default: None
Options: 3 to 128 bits
Function: Specifies the length of the prefix (in bits) associated with the IPv6 address of this entry. A prefix can not be shorter than 3 bits.
Instructions: Supply the length of the prefix that you specified with the Interface Prefix parameter.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.6

Parameter: Routing Preference

Path: Configuration Manager > Protocols > IPv6 > List Prefixes
Default: 15
Options: 1 to 15
Function: Supplies a preference value for this prefix
Instructions: Supply a preference value from 0 to 15 (most preferred).
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.7

Parameter: Prefix Cost

Path: Configuration Manager > Protocols > IPv6 > List Prefixes
Default: 1
Options: 1 to 15
Function: Specifies the cost metric associated with this entry. (This value is used as the RIP metric.)
Instructions: Supply an integer from 1 (default) to 15.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.8

Parameter: On Link Flag

Path: Configuration Manager > Protocols > IPv6 > List Prefixes
Default: On
Options: On │ Off
Function: Specifies whether this prefix can be used for on-link determination.
Instructions: Set this parameter as required for the prefix.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.9

Parameter: **Autonomous Prefix Flag**

Path: Configuration Manager > Protocols > IPv6 > List Prefixes

Default: On

Options: On │ Off

Function: Controls the autonomous address configuration flag.

Instructions: Turn the flag On to indicate that this prefix can be used for autonomous address configuration -- that is, the prefix can be used to form a local interface address.

If you turn the flag OFF, the prefix is not used to form a local interface address but is advertised in neighbor discovery router advertisements.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.10

Parameter: **Relative Preferred Lifetime**

Path: Configuration Manager > Protocols > IPv6 > List Prefixes

Default: 604800 seconds

Options: An integer expressing the number of seconds

Function: Supplies a value for the preferred lifetime field in the prefix information option of a router advertisement. This parameter indicates the length of time in seconds (relative to the time the router advertisement is sent) that this prefix will remain preferred -- that is, the time until deprecation. A value of 0xffffffff represents infinity.

Instructions: When the preferred lifetime expires, the address generated from a deprecated prefix should no longer be used as a source address in new communications. However, packets received on such an interface are processed as expected.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.11

Parameter: **Relative Valid Lifetime**

Path: Configuration Manager > Protocols > IPv6 > List Prefixes

Default: 0xffffffff (-1)

Options: An integer representing the number of seconds

Function: Specifies a value to be placed in the valid lifetime field in the prefix information option of router advertisements. This parameter indicates the length of time in seconds (relative to the time the router advertisement is sent) that this prefix will remain valid -- that is, the time until invalidation. A value of 0xffffffff (-1) represents infinity.

Instructions: The address generated from an invalidated prefix should not appear as the destination or source address of a packet.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.3.1.12

IPv6 Neighbor Discovery Parameters

Parameter: **Enable**

Path: Configuration Manager > Protocols > IPv6 > List Neighbor Discovery

Default: Enable

Options: Enable │ Disable

Function: Enables and disables this neighbor discovery interface.

Instructions: Set this parameter as required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.3.1.1. 2

Parameter: **Router Advertisement**

Path: Configuration Manager > Protocols > IPv6 > List Neighbor Discovery

Default: Off

Options: On │ Off

Function: Indicates whether or not periodic route advertisements are to be sent.

Instructions: If you want IPv6 to send route advertisements, turn this parameter on.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.3.1.1.5

Parameter: Managed Address Configuration

Path: Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default: Off
Options: On │ Off
Function: Manages the address configuration flag.
Instructions: Turn this flag on if you want hosts to use the administered (stateful) protocol for address autoconfiguration in addition to any addresses autoconfigured using stateless address autoconfiguration.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.3.1.1.6

Parameter: Managed Non-Address

Path: Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default: Off
Options: On │ Off
Function: Manages the stateful configuration flag for autoconfiguration of nonaddress information.
Instructions: Turn this flag on if you want hosts to use the administered (stateful) protocol for autoconfiguration of nonaddress information.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.3.1.1.7

Parameter: Reachable Time

Path: Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default: 0
Options: An integer
Function: Specifies the time, in milliseconds, that a node assumes a neighbor is reachable after having received a reachability confirmation. A value of 0 means the reachable time is unspecified by this router.
Instructions: Specify a reachable time for this neighbor.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.3.1.1.8

Parameter: Retransmission Time

Path:	Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default:	0
Options:	An integer
Function:	Specifies the time, in milliseconds, between retransmitted neighbor solicitation messages. A value of 0 means the retransmission time is unspecified by this router.
Instructions:	Supply a transmission for this neighbor connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.3.1.1.9

Parameter: Maximum Hop Limit

Path:	Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default:	64
Options:	0 to 255
Function:	Specifies a maximum hop limit (network diameter) to advertise.
Instructions:	Supply a hop limit for this neighbor connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.3.1.1.10

Parameter: Minimum Multicast

Path:	Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default:	200 seconds
Options:	3 to 1350 seconds
Function:	Specifies the minimum time (in seconds) allowed between sending unsolicited multicast router advertisements.
Instructions:	Supply a minimum multicast time for this neighbor connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.3.1.1.11

Parameter: Maximum Multicast

Path:	Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default:	600
Options:	4 to 1800
Function:	Specifies the maximum time (in seconds) allowed between sending unsolicited multicast router advertisements.
Instructions:	Specify a maximum multicast time for this neighbor connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.3.1.1.12

Parameter: Default Lifetime

Path:	Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default:	1800 seconds
Options:	0 to 9000 seconds
Function:	Specifies the lifetime (the number of seconds) associated with the default router.
Instructions:	Specify a default router lifetime for this neighbor connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.3.1.1.13

Parameter: Duplicate Address Detection

Path:	Configuration Manager > Protocols > IPv6 > List Neighbor Discovery
Default:	1
Options:	0 to 10
Function:	Specifies the number of consecutive neighbor solicitation messages sent while performing duplicate address detection on a tentative address. A value of 0 indicates that no duplicate address detection needs to be performed. A value of 1 indicates a single transmission with no follow-up retransmission.
Instructions:	Configure duplicate address detection for this neighbor connection.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.3.1.1.14

IPv6 Adjacent Node Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IPv6 > List Adjacent Nodes
Default: Enable
Options: Enable │ Disable
Function: Enables and disables this adjacent node definition.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.7.1.2

Parameter: Physical Address

Path: Configuration Manager > Protocols > IPv6 > List Adjacent Nodes
Default: None
Options: See below.
Function: Supplies the physical address of this adjacent node. For a frame relay PVC, this address is a 32-bit DLCI. For an ATM PVC this address is a 32-bit VCID which has circuit VCI in its 20 most-significant bits and VPI in its 12 least-significant bits.
Instructions: You must supply a physical address for this adjacent node definition.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.7.1.5

Parameter: Link Layer Encapsulation

Path: Configuration Manager > Protocols > IPv6 > List Adjacent Nodes
Default: other
Options: other │ snap (IEEE 802.2) │ pdn (X.25 PDN) │ wan (FR SVC, ATM SVC)
Function: Specifies the link layer encapsulation type of this entry.
Instructions: Specify SNAP encapsulation only if IEEE 802.2 encapsulation is to be used over CSMACD or DS1 links.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.7.1.6

Parameter: Routing Preference

Path:	Configuration Manager > Protocols > IPv6 > List Adjacent Nodes
Default:	15 (most preferred)
Options:	1 to 15
Function:	Specifies a routing preference value from 0 to 15.
Instructions:	You must specify a routing preference for this adjacent node definition.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.7.1.7

Parameter: Cost

Path:	Configuration Manager > Protocols > IPv6 > List Adjacent Nodes
Default:	1
Options:	1 to 15
Function:	Supplies a cost for the this adjacent node definition. (The value is used as the RIP metric.)
Instructions:	You must specify a cost for this adjacent node definition.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.7.1.8

Parameter: X.121 Address

Path:	Configuration Manager > Protocols > IPv6 > List Adjacent Nodes
Default:	None
Options:	A WAN address
Function:	Supplies a WAN address (for example, an X.121 or E.164 address) to establish an SVC to the adjacent host. For an X.25 PVC, this parameter contains the LCN of the PVC encoded as an X.121 address up to 4 octets in length.
Instructions:	Supply the appropriate address for your network.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.7.1.10

IPv6 Static Route Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IP6 > List Static Routes
Default: Enable
Options: Enable | Disable
Function: Enables and disables this static route.
Instructions: Set this parameter as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.6.1.2

Parameter: Prefix

Path: Configuration Manager > Protocols > IPv6 > List Static Routes
Default: None
Options: An IPv6 address prefix
Function: Supplies the destination IPv6 address prefix of this static route.
Instructions: You must supply an IPv6 address prefix for the static route definition.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.6.1.5

Parameter: Prefix Length

Path: Configuration Manager > Protocols > IPv6 > List Static Routes
Default: None
Options: 0 to 128 bits
Function: Supplies the length (in bits) of the address prefix for this static route.
Instructions: Indicate the length of the prefix you supplied with the Prefix parameter.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.1.6.1.6

Parameter: Next Hop Address

Path:	Configuration Manager > Protocols > IPv6 > List Static Routes
Default:	None
Options:	An IPv6 address
Function:	Supplies the IPv6 address of the next-hop node.This parameter is ignored for a black hole static route.
Instructions:	You must supply an IPv6 address for the static route definition.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.6.1.7

Parameter: Route Preference

Path:	Configuration Manager > Protocols > IPv6 > List Static Routes
Default:	15 (most preferred)
Options:	0 to 15
Function:	Supplies a routing preference value from 0 to 15.
Instructions:	You must supply a routing preference value for the static route definition.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.6.1.8

Parameter: Cost

Path:	Configuration Manager > Protocols > IPv6 > List Static Routes
Default:	1
Options:	1 to 15
Function:	Specifies the cost of this static route. (This value is used as the RIP metric.)
Instructions:	You must supply a cost value for the static route definition.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.1.6.1.9

RIP IPv6 Interface Parameters

Parameter: Enable

Path: Configuration Manager > Protocols > IPv6 > RIPv6>Interfaces
Default: Enable
Options: Enable │ Disable
Function: Enables and disables this RIPv6 interface
Instructions: Set the state of the IPv6 interface as required.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1. 2

Parameter: RIP Supply

Path: Configuration Manager > Protocols > IPv6 >RIPv6>Interfaces
Default: Enable
Options: Enable │ Disable
Function: Specifies whether the interface transmits periodic RIP updates to neighboring networks.
Instructions: Select Enable to configure the interface to transmit RIP updates. Select Disable to prohibit the interface from transmitting RIP updates.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.5

Parameter: RIP Listen

Path: Configuration Manager > Protocols > IPv6 >RIPv6>Interfaces
Default: Enable
Options: Enable │ Disable
Function: Specifies whether this interface listens to RIP updates from neighboring networks.
Instructions: Select Enable to configure this interface to listen to RIP updates and, thus, add received routing information to its internal routing table. If you select Enable, a configured policy can still prohibit the interface from updating its internal routing table. Select Disable to configure the interface to ignore RIP updates from neighboring routers. Thus, the interface does not add received routing information to its internal routing table.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.6

Parameter: Default Route Supply

Path: Configuration Manager > Protocols > IPv6 >RIPv6>Interfaces

Default: Disable

Options: Enable │ Disable │ Generate

Function: Specifies whether or not the interface advertises a default route in RIP updates sent to neighboring networks. When a router does not know the route of a particular address, it uses the default route as the destination. A configured policy can override this setting. This parameter is independent of the RIP Supply parameter.

Instructions: If you select Enable, RIP advertises the default route if it is present in the routing table -- that is, if you have statically included a default route in the table or if the router has learned the default route (0.0.0.0) dynamically. If you select Generate, RIP advertises a default route whether or not a default route is present in the routing table. (This parameter does not cause RIP to create a routing table entry for a default route; the route will not be visible in the routing table.)

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.7

Parameter: Default Route Listen

Path: Configuration Manager > Protocols > IPv6 > RIPv6>Interfaces

Default: Disable

Options: Enable │ Disable

Function: Specifies whether or not IP adds default route information to its internal routing table.

Instructions: Select Enable to configure the RIP interface to listen for and potentially add the default route (0.0.0.0) information to its internal routing table. Note that you must also enable RIP Listen on this interface. A configured policy can override this setting. Select Disable to prohibit the RIP interface from adding the default route (0.0.0.0) information to its internal routing table.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.8

Parameter: Poison

Path: Configuration Manager > Protocols > IPv6 > RIPv6>Interfaces

Default: Poisoned

Options: Poisoned │ Actual │ Split

Function: Specifies how the RIP interface advertises routes it learns from an adjacent network in periodic updates subsequently sent to that network.

Instructions: Select Poisoned to configure this RIP interface to implement poisoned reverse. When poisoned reverse is enabled, the RIP interface advertises routes to the adjacent network from which it has learned the routes. In RIP updates, RIP uses a hop count of RIP Network Diameter plus one, thus declaring the destination unreachable. Poisoned reverse can speed up the convergence of the network routing tables. Select Split to configure this RIP interface to implement a split horizon. When split horizon is enabled, the RIP interface omits routes learned from a neighbor in RIP updates subsequently sent to that neighbor. Select Actual to configure this RIP interface to advertise routes with the learned cost. This is useful on a frame relay interface that has virtual connections (VCs) to different routers that are part of the same logical IP subnet.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.9

Parameter: Broadcast Timer

Path: Configuration Manager > Protocols > IPv6 >RIPv6>Interfaces

Default: 30 seconds; 1 hour for dial-optimized routing

Options: 5 seconds to 86,400 seconds (24 hours); 1 hour to 1,209,600 seconds (2 weeks) for dial-optimized routing

Function: Specifies how frequently RIP does a full update of the routing table.

Instructions: Enter a value in 5-second increments.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.10

Parameter:	**Timeout Timer**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6> Interfaces
Default:	90 seconds; 3 hours for dial-optimized routing
Options:	15 to 259,200 seconds (72 hours); 3 hours to 3,628,800 seconds (6 weeks) for dial-optimized routing
Function:	Specifies the time period that RIP will wait for an update for a particular network before declaring it to be unreachable.
Instructions:	We recommend a timeout value of the broadcast time multiplied by 3. Enter a time in 5-second increments.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.11

Parameter:	**Hold Down Timer**
Path:	Configuration Manager > Protocols > IPv6 > List RIP Interfaces
Default:	90 seconds; 3 hours for dial-optimized routing
Options:	15 to 259,200 seconds (72 hours); 3 hours to 3,628,800 seconds (6 weeks) for dial-optimized routing
Function:	Specifies the time period that unusable routes will be advertised through this interface after the route has become invalid.
Instructions:	We recommend a timeout value of the broadcast time multiplied by 3. Enter a time in 5-second increments. This parameter affects how long a route remains in the routing table after the route has become unusable. To guarantee the holddown time for each interface, RIP uses the largest holddown value as the amount of time to keep the route in the routing table. Please note that if a route to a destination becomes unusable, the holddown value will not affect the router's ability to learn new routes to the same destination.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.12

Parameter: **Triggered Updates**

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Interfaces

Default: Disable

Options: Enable | Disable

Function: Configures RIP to generate an update each time it recalculates a route's metric.

Instructions: If you enable triggered updates, RIP will generate triggered updates with a maximum frequency of one every 5 seconds. The route will include all changes that occurred in the last 5 seconds. This enforced interval prevents RIP from monopolizing CPU resources during periods of instability.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.13

Parameter: **RIP Diameter**

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Interfaces

Default: 15

Options: 0 to 15

Function: Specifies the value, or hop count, that RIP uses to denote infinity.

Instructions: You must set this parameter so that none of the interface cost, static cost, or route filter cost parameters exceed the RIP diameter. We recommend that you accept the default RIP diameter value of 15.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.1.2.1.1.14

RIPv6 Accept Policy Parameters

Parameter: **Accept Enable**

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept

Default: Enable

Options: Enable | Disable

Function: Enables and disables this policy

Instructions: Set the parameter as required.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.1.1.2

Parameter: Accept Name

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept
Default: None
Options: Text string
Function: Specifies a user name for the policy.
Instructions: Enter a unique name for this policy.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.1.1.4

Parameter: Accept Prefixes

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept
Default: Null
Options: See below.
Function: Prefix identification list. This identifies which prefixes will match this rule. If non-null, the octet string contains one or more 3-tuples of the following form:

First octet: exact (1) or range (2)
Next 16 octets: prefix
Next octet: prefix length

Instructions: An entry with an “exact” tag means to only match the specific network advertisement (prefix and length). An entry with a “range” tag means to match any prefix that falls in the range indicated by the prefix and length.

An “exact” encoding of ::0/128 means match the default route. A “range” encoding of ::0/0 means match any route.

A null string also means match any route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.1.1.5

Parameter: Accept Action

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept

Default: Accept

Options: Accept | Ignore

Function: Specifies the action taken if the route matches this policy.

Instructions: Select Accept if you want the route to be considered for inclusion in the routing table.

Select Ignore if you want to drop the route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.1.1.6

Parameter: Accept Preference

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept

Default: 1

Options: 1 to 15

Function: Supplies a metric to be used to compare the route to other routes to the same destination.

Instructions: A value of 15 is “most preferred.” This parameter has meaning only if the action is Accept.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.1.1.7

Parameter: Accept Precedence

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept

Default: Null

Options: An integer indicating the precedence of the route

Function: Supplies a metric to be used to compare this policy rule to other rules that a given route may match.

Instructions: A rule with a higher precedence value will be chosen over one with a smaller value. In the case of a tie, the rule index is used (larger wins).

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.1.1.8

Parameter:	**Accept Inject**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept
Default:	Null
Options:	See below.
Function:	Inserts prefixes into the routing table that differ from the actual advertised prefixes.
Instructions:	This octet string should be non-null only if the action is Accept and if you want to insert prefixes into the routing table that differ from the actual advertised prefixes. For instance, if a number of prefixes in a certain range are learned, an aggregate advertisement could be inserted instead of the individual prefixes. If non-null, The octet string contains one or more 2-tuples of the following form: First 16 octets: prefix Next octet: prefix length Upon receiving a route that matches this filter, all prefixes in this list will be considered for inclusion in the routing table. If the list is null, the actual received network is considered. An encoding of ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 means “match the actual received prefix.” This allows the insertion of an aggregate or default along with the actual prefix. This parameter will be used only for routes received via RIP.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.1.1.9

Parameter:	**Accept Gateway**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept
Default:	Null
Options:	See below.
Function:	If non-null, the octet string contains one or more 4-octet interface indexes with the following format: First 4 octets: interface index Next 16 octets: router address ::0 means any address. If null, this policy applies to RIP updates received on any interface.
Instructions:	If non-null, the octet string contains one or more 4-octet interface indexes. If null, this filter applies to RIP updates received on any interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.1.1.10

Parameter:	**Accept Interface**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept
Default:	Null
Options:	See below.
Function:	Supplies a RIP interface list -- an octet string that contains the addresses of one or more interfaces on this router. If an interface address is included in this list, this policy applies to RIP advertisements received on that interface.
Instructions:	If you supply an octect string, the octet string must contain one or more 4-octet interface indexes. If null, this policy applies to RIP updates received on any interface.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.1.1.11

Parameter:	**Accept Log**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Accept
Default:	False
Options:	True | False
Function:	Specifies a log action. If True, a log event is generated when a prefix matches this policy rule; if False, no logging is done.
Instructions:	If you want to generate a log message when a prefix matches this policy, set the parameter to True.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.1.1.12

RIPv6 Announce Policy Parameters

Parameter:	**Announce Enable**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default:	Enable
Options:	Enable | Disable
Function:	Enables and disables this announce policy.
Instructions:	Set the parameter as required.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.2.1.2

Parameter:	**Announce Name**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default:	None
Options:	Text string
Function:	Specifies a user name for the policy.
Instructions:	Enter a unique name for this policy.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.2.1.4

Parameter: Announce Prefixes

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce

Default: Null

Options: See below.

Function: Prefix identification list. This identifies which prefixes will match this rule. If non-null, The octet string contains one or more 3-tuples of the following form:

First octet: exact (1) or range (2)
Next 16 octets: prefix
Next octet: prefix length

Instructions: An entry with an “exact” tag means to only match the specific network advertisement (prefix and length). An entry with a “range” tag means to match any prefix that falls in the range indicated by the prefix and length.

An “exact” encoding of ::0/0 means match the default route. A “range” encoding of ::0/0 means match any route.

A null string also means match any route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.5

Parameter: Announce Action

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce

Default: Announce

Options: Announce | Ignore

Function: Specifies the action taken if the route matches this policy.

Instructions: Select Announce if you want the route to be advertised.

Select Ignore if you want to drop the route.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.6

Parameter: Announce Precedence

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default: Null
Options: An integer indicating the precedence of route
Function: Supplies a metric to be used to compare this policy rule to other rules that a given route may match.
Instructions: A rule with a higher precedence value will be chosen over one with a smaller value. In the case of a tie, the rule index is used (larger wins).
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.7

Parameter: Announce Route Source

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default: Any
Options: Direct | Static | RIP | OSPF | BGP | Any
Function: Supplies one or more route source identifiers. If the route source is in this list, then a route from that source that meets the other criteria of this policy will match the policy.
Instructions: Specify one or more route sources.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.8

Parameter: Announce External Route Source

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default: Any
Options: Direct | Static | RIP | OSPF |BGP | Any
Function: Supplies one or more route source identifiers. If the route source is in this list, then a route from that source that meets the other criteria of this policy will match the policy.
Instructions: Specify one or more route sources.
MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.9

Parameter:	**Announce Advertise**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default:	Null
Options:	See below.
Function:	Advertises networks that differ from the actual advertised prefixes.
Instructions:	this octet string should be non-null only if the action is Announce and if you want to advertise networks that differ from the actual network in the routing table. For instance, if a number of networks in a certain range are in the table, an aggregate could be advertised instead of the individual networks. If non-null, the octet string contains one or more 2-tuples of the following form: First 16 octets: prefix Next octet: prefix length Upon receiving a route that matches this filter, all prefixes in this list will be considered for inclusion in the routing table. If the list is null, the actual received network is considered. An encoding of ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 means match the actual received prefix. This allows advertisement of an aggregate or default along with the actual prefix. This parameter will be used only for routes received via RIP.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.2.1.10

Parameter: Announce RIP Gateway

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce

Default: Null

Options: See below.

Function: Supplies a “from RIP” gateway list. This parameter is applicable only for RIP sourced routes and if RIP is included as a route source.

Instructions: This octet string contains the addresses of one or more routers that could send RIP updates to this router. If a router address is included in this list, this filter applies to RIP advertisements from that router.

If non-null, the octet string contains one or more 2-tuples of the following form:

First 4 octets: interface index
Next 16 octets: router address

::0 means any address.

If null, this filter applies to RIP updates from any router.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.11

Parameter: Announce Interface

Path: Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce

Default: Null

Options: See below.

Function: Supplies a RIP outbound interface list -- an octet string that contains the addresses of one or more interfaces on this router. If an interface address is included in this list, this policy applies to RIP advertisements received on that interface.

Instructions: If you supply an octect string, the octet string must contain one or more 4-octet interface indexes. If null, this policy applies to RIP updates received on any interface.

MIB Object ID: 1.3.6.1.4.1.18.3.5.3.16.6.2.1.12

Parameter:	**Announce RIP Metric**
Path:	Configuration Manager > Protocols > IPv6 > RIPv6 > Policies > Announce
Default:	Null
Options:	0 to 15
Function:	Supplies a RIP metric.
Instructions:	This parameter is valid only if the action is Announce. This is an optional announce parameter metric to use when advertising a route that matches this policy. If zero, the routing table metric calculated for RIP plus the interface cost is used.
MIB Object ID:	1.3.6.1.4.1.18.3.5.3.16.6.2.1.13

Index

A

actual cost update mode, 4-7

addresses
- anycast, 1-3
- IPv6, 1-2
- IPv6 next-hop, 3-65
- link layer, 3-13
- local IPv4, 3-27
- MAC, 3-13
- multicast, 1-3
- physical, for adjacent node, 3-56
- prefix for, enabling and disabling, 3-33
- remote IPv4, 3-28
- remote IPv6, 3-30
- SMDS group, 3-20
- WAN, 3-60

adjacent node
- cost, 3-59
- enabling and disabling, 3-55
- link layer encapsulation type, 3-57
- physical address for, 3-56
- route preference value, 3-58
- WAN address of, 3-60

anycast addresses, 1-3

autoconfiguration
- host, 1-12

automatic tunnel, 3-25

automatic tunnels, 1-8

autonomous address configuration, 3-39

Autonomous Prefix Flag parameter, 3-39, A-13

B

Bay Networks Press, xviii

Broadcast Time parameter, 4-8

Broadcast Timer parameter, A-24

C

Cache Size parameter, 3-15, A-5

circuit name for IPv6, 3-12

Circuit Name parameter, 3-12, 3-24, A-4

circuitless interface
- specifying slots for, 3-16

configured tunnels, 1-6

cost
- adjacent node, 3-59

Cost parameter
- adjacent node, 3-59, A-19
- static route, 3-67, A-21

customer support
- programs, xix
- Technical Solutions Centers, xix

D

Default Hop parameter, A-2
- IPv6, 3-4

Default Lifetime parameter, 3-52, A-17

default route
- listening for, 4-6
- supplying, 4-5

Default Route Listen parameter, 4-6, A-23

Default Route Supply parameter, 4-5, A-23

describing IPv6 interface, 3-10

diameter
RIP, 4-12
disabling
address prefixes, 3-33
adjacent node, 3-55
autonomous address configuration, 3-39
global IPv6, 3-2
IPv6 interface, 3-9
MTU Path Discovery, 3-6
Neighbor Discovery, 3-43
redirect messages, 3-17
RIP, 4-2
static route, 3-62
TR end station support, 3-19
Duplicate Address Detection parameter, 3-53, A-17

E

Enable parameter
adjacent node, 3-55, A-18
global, A-1
global IPv6, 3-2
IPv6 prefix, 3-33
IPv6 interface, 3-9, A-3
neighbor discovery, 3-43, A-14
prefix, A-11
RIP Interface, 4-2
RIP interface, A-22
static route, 3-62, A-20
enabling
address prefixes, 3-33
adjacent node, 3-55
autonomous address configuration, 3-39
global IPv6, 3-2
IPv6 interface, 3-9
MTU Path Discovery, 3-6
Neighbor Discovery, 3-43
redirect messages, 3-17
RIP, 4-2
static route, 3-62
TR end station support, 3-19
end station
token ring, 3-19
extension headers, 1-11

F

format
IPv6 address, 1-2, 1-4
multicast address, 1-3
Forwarding parameter, 3-3, A-1
forwarding table
specifying size of, 3-15
Frame Relay Broadcast DLCI parameter, 3-21, A-7
Frame Relay Multicast DLCI #1 parameter, 3-22, A-7
Frame Relay Multicast DLCI #2 parameter, 3-22, A-7

H

header, IPv6, 1-1
Hold Down Timer parameter, 4-10, A-25
hop limit, 3-4
host autoconfiguration, 1-12

I

ICMP error messages, 3-18
index
local IPv6, 3-29
Interface Description parameter, 3-10, A-3
Interface Prefix parameter, 3-34, A-11
Interface Token parameter, 3-11, A-4
interval
update broadcast, 4-8
IPv4
local address, 3-27
remote address, 3-28
IPv6
addresses, 1-2

circuit name, 3-12
endpoint of a tunnel, 3-24
extension headers, 1-11
global
enabling and disabling, 3-2
header, 1-1
interface
enabling and disabling, 3-9
local index, 3-29
packet forwarding, 1-10
remote address, 3-30
starting, 2-1
tunnels, 1-6
IPv6 hop limit, 3-4
IPv6 interface
describing, 3-10
IPv6 Local Index parameter, 3-29, A-10

L

link layer address, 3-13
Link Layer Address parameter, 3-13, A-4
Link Layer Encapsulation parameter, 3-57, A-18
Link MTU parameter, 3-14, A-5
link MTU size, 3-5, 3-14
listening for default route, 4-6

M

MAC address, 3-13
Managed Address Configuration parameter, 3-45, A-15
Managed Non-Address parameter, 3-46, A-15
Max ICMP Messages parameter, 3-18, A-6
Maximum Hop Limit parameter, 3-49, A-16
Maximum Multicast parameter, 3-51, A-17
messages
ICMP error, 3-18
redirect, 3-17
Minimum Link MTU parameter, 3-5, A-2
Minimum Multicast parameter, 3-50, A-16
MTU Discovery parameter, A-2
IPv6, 3-6
MTU Path Discovery
enabling and disabling, 3-6
timout value for, 3-7
MTU Timeouts parameter, 3-7, A-3
multicast addresses, 1-3

N

naming IPv6 circuit, 3-12
neighbor discovery (ND), 1-12
address autoconfiguration, 3-45
detecting duplicate addresses, 3-53
enabling and disabling, 3-43
lifetime for default router, 3-52
maximum hop limit for advertisements, 3-49
maximum time for unsolicited advertisements, 3-51
minimum time for unsolicited advertisements, 3-50
neighbor reachability time for, 3-47
retransmission time for, 3-48
router advertisements, 3-44
network, unreachable
advertising a route to, 4-10
timeout period for, 4-9
Next Hop Address parameter, 3-65, A-21
next-hop address for IPv6, 3-65

O

On Link Flag parameter, 3-38, A-12

P

packet forwarding, 1-10
Physical Address parameter, 3-56, A-18
Poison parameter, 4-7, A-24

poisoned reverse update mode, 4-7
prefix
  cost, 3-37
  enabling and disabling, 3-33
  length of, 3-35
  on-link determination, 3-38
  preference value, 3-36
  preferred lifetime, 3-40
  supplying, 3-34
  valid lifetime, 3-41
Prefix Cost parameter, 3-37, A-12
Prefix Length parameter, 3-35, 3-64, A-11
  static route, A-20
Prefix parameter, 3-63, A-20
publications, ordering, xviii

R

Reachable Time parameter, 3-47, A-15
receiving RIP updates, 4-4
redirect messages
  enabling and disabling, 3-17
Redirect On/Off parameter, 3-17, A-6
Relative Preferred Lifetime parameter, 3-40, A-13
Relative Valid Lifetime parameter, 3-41, A-14
Retransmission Time parameter, 3-48, A-16
RIP
  diameter, 4-12
  enabling and disabling, 4-2
  receiving updates, 4-4
  supplying updates, 4-3
RIP Diameter parameter, 4-12, A-26, A-27, A-28, A-29, A-30, A-31, A-32, A-33, A-34, A-35, A-36
RIP Listen parameter, 4-4, A-22
RIP Supply parameter, 4-3, A-22
Route Preference parameter, 3-66, A-21
Router Advertisement parameter, 3-44, A-14
Routing Preference parameter
  adjacent node, 3-58, A-19
  IPv6 prefix, 3-36
  prefix, A-12

S

semiautomatic tunnel, 1-10, 3-25
sending triggered updates, 4-11
size
  forwarding table, 3-15
  link MTU, 3-5, 3-14
Slot Mask parameter, 3-16, A-5
slots, specifying for circuitless interface, 3-16
SMDS group address, 3-20
SMDS Group Address parameter, 3-20, A-7
split horizon update mode, 4-7
starting IPv6, 2-1
stateful host autoconfiguration, 1-12
stateless host autoconfiguration, 1-12
static route
  associating with an interface, 3-61
  destination IPv6 address prefix, 3-63
  enabling and disabling, 3-62
  next-hop address, 3-65
  prefix length, 3-64
static tunnel, 1-6, 3-25

supplying
default route, 4-5
RIP updates, 4-3

T

Technical Solutions Centers, xix
timeout
MTU Path Discovery, 3-7
unreachable network
timeout period for, 4-9
Timeout Timer parameter, 4-9, A-25
timer
hold down, 4-10
TR End Station parameter, 3-19, A-6
TR end station support, enabling and disabling, 3-19
triggered updates
sending, 4-11
Triggered Updates parameter, 4-11, A-26
Tunnel IPv4 Local Address parameter, 3-27, A-9
Tunnel IPv4 Remote Address parameter, 3-28, A-9
Tunnel IPv6 Remote Address parameter, 3-30, A-10
Tunnel Protocol Type parameter, 3-26, A-8
tunnels, 1-6
automatic, 1-8
configured, 1-6
configuring IPv6 as endpoint, 3-24
semi-automatic, 1-10
static, 1-6
types of, 3-25

U

unreachable network
advertising a route to, 4-10
unreachable network timeout period, 4-9
upates
receiving RIP, 4-4
update modes, specifying, 4-7
updates
supplying RIP, 4-3
triggered, 4-11

W

WAN address of adjacent node, 3-60

X

X.121 Address parameter, 3-60, A-19